Российский государственный гуманитарный университет
Russian State University for the Humanities

RSUH/RGGU BULLETIN
№ 12 (155)

Academic Journal

Series:
Records Management and Archival Studies.
Computer Science.
Data Protection and Information Security

Moscow
2015

ВЕСТНИК РГГУ
№ 12 (155)

Научный журнал

Серия
«Документоведение и архивоведение.
Информатика. Защита информации
и информационная безопасность»

Москва
2015

УДК 651.4(05)+930.25(05)+004(05)
ББК 65.050.2я5+79.3я5+32.81я5

Ответственный за выпуск: С.Т. Петров (РГГУ)

ISSN 2073-6371

СОДЕРЖАНИЕ

Информатика, защита информации и информационная безопасность

Документоведение и архивоведение

Рецензии

События

CONTENTS

Computer Science, Data Protection and Information Security

Records Management and Archival Studies

Reviews

Events

О.В. Казарин, Р.А. Шаряпов

ВРЕДОНОСНЫЕ ПРОГРАММЫ НОВОГО ПОКОЛЕНИЯ – ОДНА ИЗ СУЩЕСТВЕННЫХ УГРОЗ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализ событий последних трех-четырех лет говорит о том, что эпоха кибервойн началась. Разработка и применение таких вредоносных программ, как Stuxnet, Flame, Duqu, Gauss, Wiper, Shamoon, Regin, позволяет констатировать тот факт, что начались если не сами кибервойны, то широкомасштабные диверсионно-разведывательные кибероперации, проводимые государственными структурами против критически важных объектов других государств. А это само по себе и может являться предвестником кибервойн. Характер, особенности проведения таких кибероперации и связанные с этим проблемы, разрабатываемые вредоносные программы и являются предметом исследования настоящей статьи.

Решение задач по обнаружению и нейтрализации вредоносных программ необходимо проводить как в рамках национальных систем противодействия компьютерным атакам, так и в рамках системы международной информационной безопасности, способной решать подобные задачи на политико-дипломатическом, правовом, технологическом и организационном направлениях. Предложения по проведению мероприятий в рамках создания и эволюционирования такой системы также рассматриваются в настоящей работе.

Ключевые слова: киберпространство, кибервойны, информационно-коммуникационные технологии, информационное оружие, вредоносные программы, международная информационная безопасность.

Введение

Появление и применение вредоносных программ[1] Stuxnet, Flame, Duqu, Gauss, Wiper, Shamoon, Regin и их разновидностей, по большому счету, явилось прецедентом (на взгляд авторов, неоспоримым фактом) *начала эпохи кибервойн, широкомасштабных кибероперaций*[2]. При этом большинство экспертов относят эти программы к *разновидностям информационного оружия*, которое применялось (применяется) для[3,4,5]:

- Stuxnet – деструктивного воздействия на автоматизированные системы управления комплексом по обогащению урана в Натанзе[6] (Иран);
- Shamoon – деструктивного воздействия на ключевые нефтегазовые компании энергетической инфраструктуры на Ближнем Востоке (Saudi Aramco, Саудовская Аравия и Ras Gas, Катар);
- Flame, Duqu, Gauss – организации утечки конфиденциальной информации о критически важных объектах и даже конкретных учреждениях и персоналиях, имеющих отношение к ракетной и ядерной программе Ирана и других ближневосточных стран;
- Wiper – удаление конфиденциальных данных с компьютеров правительства Ирана.

Детальный анализ, проведенный специалистами многих антивирусных компаний, таких, например, как «Лаборатория Касперского», Symantec и др., говорит о том, что вести такие кибервойны[7] или, точнее, такие «мощные» кибероперации[8] под силу только государственным структурам или организациям, действующим в тесном взаимодействии с ними, причем действовавшим не только в киберпространстве, но и осуществлявшим агентурное прикрытие и обеспечение подобных кибердействий[9].

В ближайшем будущем следует ожидать других примеров *применения кибероружия, возможно, даже более разрушительного,* чем указанное выше.

Так, в конце 2014 г. одновременно появились сообщения от разных антивирусных компаний о возникновении новой вредоносной программы Regin, которая нацелена не только на конкретные корпоративные цели, в том числе на критически важные объекты в конкретных странах, но и на информационные системы целых стран и групп стран. Предположительно Regin атакует компании связи и интернет-провайдеров в России, Саудовской Аравии, Мексике и Иране.

Таким образом, речь уже может идти о начале эпохи кибервойн. Хотя здесь возникает целый ряд вопросов и на некоторые из них пока нет ответов:

- насколько политический и военный эффект от проведения подобных кибероперациий соответствует их замыслу?
- может все же это – демонстрация возможностей, устрашение, «проба пера» или что-то подобное?
- насколько затраты (временные, финансовые, «людские», интеллектуальные) будут сопоставимы с наносимым ущербом для объекта кибератаки и следует ли вообще ожидать результатов от такого сопоставления?[10]
- насколько такая широкая избирательность / неизбирательность, например, Regin позволяет ее заказчикам / создателям достигать своих целей / решать свои задачи?

Ведь если бы Stuxnet нанес заводу в Натанзе значительный ущерб, то обогащение урана замедлилось бы. Однако отчеты МАГАТЭ говорят об обратном: в период с 2007 по 2013 г. количество урана, обогащенного на нем, равномерно росло. Обогащение до 20% началось как раз в тот период, когда часть центрифуг была выведена из строя.

Подобного рода кибероперации, по большому счету, должны (могут) проводиться в рамках доктринальных документов[11] в области защиты национальных секторов киберпространства, а также в области информационного противоборства, принятых буквально за последние три-четыре года[12].

1. Некоторые доктринальные установки США и НАТО

В контексте настоящего исследования представляют интерес *следующие доктринальные документы, существенно влияющие на стратегию и тактику кибервойн*:

- Международная стратегия для киберпространства США «Процветание, безопасность и открытость сетевого мира»[13];
- Стратегия Министерства обороны США по ведению операций в киберпространстве[14];
- Стратегическая концепция НАТО «Активное вовлечение, современная защита» (Брюссель, ноябрь 2010 г.)[15].

Практически во всех этих документах кибервойны все чаще рассматриваются как стратегическая проблема государственной важности, имеющая далекоидущие последствия. А политико-технологические мероприятия некоторых государств по подготовке и

ведению таких войн являются сегодня одним из главных векторов превентивного обеспечения национальной безопасности, давления на другие страны с целью достижения геополитического, геостратегического, геоинформационного превосходства.

Президент Соединенных Штатов Америки Б. Обама в мае 2011 г. подписал Международную стратегию для киберпространства. Этот документ представляет большой интерес для понимания современной глобальной американской политики. В опубликованной стратегии наблюдается значительный пересмотр официальных позиций Соединенных Штатов по вопросам информационной безопасности.

В Стратегии декларируется, что США готовы использовать *«все необходимые средства» для защиты своих жизненно важных киберобъектов*, что США будут «отвечать на враждебные действия в киберпространстве, как и на любую другую угрозу», в том числе сохраняют за собой право *отвечать военными действиями*.

В целом в выступлениях президента США Б. Обамы, в ряде ключевых документов Белого дома содержатся упоминания, подтверждающие, что формирующаяся система международных отношений носит *полицентричный характер*. Особую роль в новом мире играют так называемые негосударственные акторы. В силу особенностей такого специфического ресурса, как информация, государство имеет ограниченные возможности управления и контроля в этой области. Однако негосударственные акторы – транснациональные корпорации, международные организации, общественные объединения, сетевые структуры – нередко обладают гораздо более мощными информационными ресурсами, чем государства. В полицентричном мире Соединенным Штатам придется конкурировать, а возможно, и противостоять различным акторам международных отношений.

Сразу бросается в глаза, что в отличие от многочисленных «национальных стратегий» документ называется «Международная стратегия для киберпространства». Очевидно, администрация США стремится использовать международное сотрудничество в области обеспечения национальной информационной безопасности.

С выходом новой стратегии кибербезопасности можно говорить о новом этапе формирования системы государственного обеспечения информационной безопасности в США. В опубликованном документе говорится о стратегическом подходе к вопросам кибербезопасности. Среди потенциальных угроз в этой сфере отмечаются как экономические, так и военные и техногенные угрозы экономике, бизнесу, обществу и национальной безопасности.

Отдельный параграф новой стратегии посвящен проблеме информационного сдерживания. В подписанной стратегии говорится

о том, что в ответ на кибератаки США готовы использовать любые средства – дипломатические, экономические и военные. Сам факт появления дискуссий об информационном сдерживании свидетельствует о том, что Соединенные Штаты *отказались от претензий на доминирование в киберпространстве, но в то же время стремятся не уступать своих позиций*.

14 июля 2011 г. военным ведомством США была представлена Стратегия Министерства обороны США по ведению операций в киберпространстве, призванная стать всеобъемлющей стратегией США *по обеспечению превосходства в киберпространстве*. Документ по-прежнему дает право США проводить *все виды военных операций в киберпространстве*[16] для нанесения «поражения и разубеждения» противника, а также предотвращения угроз национальным интересам США[17].

В оборонный бюджет США на 2014 г. был включен пункт о запуске «Инициативы кибербезопасности»[18], суть которой заключается в стремлении установить контроль над распространением кибероружия, а одна из причин – рост угроз от таких вредоносных программ, как Stuxnet. Таким образом, возможно, что в ближайшее время США предложат новую национальную стратегию или международный документ, который будет регулировать оборот кибероружия. Учитывая, что элементы кибероружия имеют форму компьютерных программ, ограничить его распространение практически невозможно. Следовательно, такой документ, если он появится, будет носить политический характер и будет направлен на ограничение круга акторов, допущенных к оборонительным и наступательным возможностям в киберпространстве.

На фоне растущих затрат на разработку кибероружия возрастает активность США по продвижению своих интересов в вопросах кибербезопасности на международном уровне.

На саммите НАТО в Лиссабоне в 2010 г. США удалось включить кибербезопасность в число приоритетных задач Стратегической концепции НАТО «Активное вовлечение, современная защита»[19] и начать выработку соглашений по кибероборонe. Таким образом, сейчас в альянсе кибератаки рассматриваются в контексте применения пятой статьи[20] Североатлантического договора[21]. Действие этой статьи фактически было расширено на нападения из киберпространства. То же самое было подтверждено и в Заявлении по итогам встречи на высшем уровне (п.п. 72, 73), обнародованном главами государств и правительств, участвовавшими в заседании Североатлантического альянса в Уэльсе 4–5 сентября 2014 г.[22]

2. Создание государственных специализированных структур для ведения кибервойн, кибероперций

Большие усилия вооруженные силы США направляют на проведение кибероперций, которые рассматриваются как одно из средств достижения информационного превосходства над любым противником, дезорганизации и вывода из строя его систем государственного, военного и гражданского управления, а также нарушения функционирования или уничтожения объектов критических инфраструктур. Американский наступательный киберпотенциал может быть использован против следующих объектов противника: военные сети командования и управления, противовоздушной обороны; военные платформы и вооружения; энергетические станции; банки и финансовые институты; транспортные информационные сети; национальные телекоммуникационные сети.

В связи с этим в США принимаются целевые программы подготовки квалифицированных кадров для ведения кибервойн. Проводятся прикладные исследования, направленные на перевод «хакерского искусства» в ремесло, доступное для рядового военнослужащего.

Аналогичные процессы идут в ряде других государств. В частности, руководство вооруженных сил Германии приступило к созданию службы сетевых операций с целью воздействия на компьютерные сети противника для использования, искажения, подмены или уничтожения информации, содержащейся в компьютерных базах данных, а также снижения эффективности их функционирования либо вывода из строя. С 30 ноября по 1 декабря 2011 г. в ФРГ прошла операция «LÜKEX 2011»[23], которая представляла собой не что иное, как учебную кибервойну. В рамках операции, в которой приняли участие не менее трех тысяч человек, имитировались массированные атаки на сайты и информационные системы ряда федеральных и региональных госучреждений. Симуляция кибервойны осуществлялась под наблюдением Национального центра кибероборонs и спецслужб, а подготовка к ней заняла почти два года.

Во Франции в 2009 г. создано государственное Сетевое и информационное агентство безопасности (FNISA – French Networks and Information Security Agency), которое будет заниматься защитой правительственных и публичных компьютерных сетей от хакерских атак. При этом планируется, что агентство будет не только защищать сети от компьютерных угроз, но и отвечать на них.

На базе ДеМонфортовского университета, находящегося в Лестере, Великобритания, была запущена программа подготовки специалистов по программированию для служб внутренней и внешней разведки MI5 и MI6. В октябре 2012 г. бывшим тогда главой Министерства иностранных дел Великобритании У. Хейгом было сделано заявление о том, что в программу набираются молодые люди, которые активно увлекаются компьютерными играми. По его словам, именно они смогут в будущем обеспечить безопасность страны.

4 сентября 2014 г. министр обороны Эстонии Свен Миксер и главнокомандующий НАТО по трансформации французский генерал Жан-Поль Паломерос подписали в ходе саммита альянса в Уэльсе договор о намерениях по созданию в Таллине учебно-тренировочного центра НАТО по кибероборонe (киберполигона). Создание учебного центра НАТО в Эстонии означает, что начнется подготовка экспертов НАТО по кибербезопасности и будут проводиться различные учения. Это увеличит присутствие альянса в Эстонии и соберет здесь международных экспертов в области кибербезопасности.

Киберполигон будет представлять собой виртуальную среду, где можно обучать руководителей и специалистов принятию стратегических решений в сфере кибербезопасности. Полигон будет организован в Таллине на базе киберполигона Сил обороны Эстонии, созданного в 2012 г. и являющегося тренировочной средой, в которой проводился ряд международных киберучений на высоком уровне. Естественным образом, нельзя исключать возможность использования данного киберполигона не только для решения задач кибероборонe, но и кибернападения. В процитированном выше Заявлении по итогам встречи на высшем уровне глав государств и правительств в сентябре 2014 г. было подтверждено, что «мы будем разрабатывать потенциал киберполигонов НАТО, основываясь в качестве первого шага на киберполигонном потенциале Эстонии, принимая во внимание при этом возможности и требования Школы систем связи и информации НАТО и других органов учебно-образовательной подготовки НАТО».

Ситуация в киберпространстве в последнее время стремительно меняется. Не исключено, что к моменту выхода этой статьи некоторые факты могут в значительной степени потерять свою актуальность. Тем не менее тенденции, характер и направленность подобных действий не вызывают сомнений в необходимости быть готовыми к оперативному и полномасштабному реагированию на угрозы использования информационных и коммуникационных технологий (ИКТ) в военных целях уже сейчас.

3. Характер и особенности ведения современных кибервойн, кибероперaций

Сегодня наряду с обычными вооруженными силами в современных войнах будут принимать участие *противостоящие друг другу кибервойска, сетевые комбатанты и даже киберпреступники и кибертеррористы*[24]. А победы и поражения в этих войнах будут носить некие виртуальные оттенки.

Для кибервойн не существует государственных границ и закрытых территорий. Они могут иметь локальный и / или глобальный характер, им свойственны высокая анонимность и скрытность действий, трудность выявления акторов и используемых ими средств.

Боевые действия в киберпространстве могут[25]:

- оказывать влияние (иногда решающее) на эффективность и успешность ведения боевых действий в других сферах, предшествовать им;
- обеспечить достижение и удержание информационного превосходства над противником, повысить их эффективность, сокращать потери и обеспечивать успешность завершения операции;
- создавать благоприятные условия для осуществления как военных, так и политических целей государства.

Особенности самого киберпространства, боевых действий в нем и их влияния на все другие сферы противоборства сторон приобретают все большее влияние и масштабы, *которые оказывают глобальное воздействие не только на эффективность операций вооруженных сил, но и на военно-политическое руководство государств, состояние экономики и проводимую политику*, так как в проведении кибероперaций могут участвовать не только боевые силы и средства, но и силы других силовых структур, гражданские средства массовой информации противоборствующих стран.

Кибервойны будут носить *многопрофильный характер общественно-экономических, военно-политических и государственных отношений*. Их целью станет не только повышение эффективности боевых действий путем завоевания информационного превосходства, но и завоевание всестороннего всеобщего превосходства над потенциальным противником или конкурентом, для решения своих экономических, политических, а если необходимо, то и военных задач.

Противостояние в киберпространстве носит, как правило или даже по определению, асимметричный характер, когда, с одной сто-

роны, может быть группа атакующих хакеров (или даже один хакер), с другой – кибервойска, «обороняющие» критически важные объекты государства. Кибервойны со стороны, например, сетевых комбатантов и / или кибертеррористов могут вестись не только против конкретных информационных объектов, но даже против целого государства, его вооруженных сил (кибервойск). Кибервойны, способы их ведения дают возможность слабой в военном отношении стороне успешно противостоять сильному противнику и даже побеждать его. Такие войны, скорее всего, будут асимметричными и иррегулярными.

На современном этапе кибервойны могут инициироваться не только государствами и правительствами, но и негосударственными организациями, «незаконными вооруженными формированиями», сетевыми комбатантами. В этом случае часто нельзя определить, какое государство или с территории какого государства ведутся кибероперации. Нет полной ясности в том, кто является противником, война это или не война.

В то же время *именно государства являются наиболее мощными субъектами, способными осуществлять разработку и применение самых современных видов кибероружия, проводить широкомасштабные кибероперации по всему миру, наносить весьма значительный урон объектам атаки, как правило, критически важным для той или иной страны* (объектам энергетического, транспортного сектора, управления и связи, возможно, объектам стратегических ядерных сил и систем, обеспечивающих их управляемость и устойчивость и т. п.).

Таким образом, на современном этапе развития человечества, когда существует сдерживание от развязывания классических, симметричных войн, огромную угрозу для безопасности многих стран представляют собой кибервойны (асимметричные, «малые» войны), ведущиеся обычным (неядерным), относительно простым и «легким» оружием, иррегулярными формированиями и способами ведения войн (операций).

Военная безопасность страны на современном этапе может быть обеспечена силами сдерживания, основу которых составляют стратегические ядерные силы, и силами, способными эффективно вести кибервойну. Первые обязаны исключить классические (симметричные) войны, а вторые – значительно ослабить, а может, и значительно сократить масштаб атакующих действий в киберпространстве.

4. Мероприятия по сдерживанию кибервойн. Международная информационная безопасность

Использование ИКТ в качестве силового разрешения межгосударственных противоречий становится все более опасной угрозой международному миру и безопасности, национальным интересам стран. Выступая на заседании Совета Безопасности Российской Федерации, посвященном вопросам противодействия угрозам национальной безопасности в информационной сфере, 1 октября 2014 г. В.В. Путин заявил: «Вместе с тем необходимо учитывать и существующие в информационной сфере риски и угрозы. Мы видим, что отдельные страны пытаются использовать свое доминирующее положение в глобальном информационном пространстве для достижения не только экономических, но и военно-политических целей»[26].

Военная политика государств должна основываться на том, что необходимо запретить вероломные методы ведения военных действий в киберпространстве[27]. Многие задачи на этом направлении должны реализовываться в рамках системы международной информационной безопасности (МИБ), к созданию которой в течение уже довольно продолжительного времени наша страна прилагает значительные усилия[28]. В «Основах государственной политики Российской Федерации в области международной информационной безопасности»[29] заложен базис формирования системы МИБ, включая, в том числе, разработку системы мер, направленных на установление международного порядка, снижающего риски использования ИКТ для осуществления враждебных действий и актов агрессии. А одной из основных угроз в области МИБ в Основах рассматривается использование ИКТ для совершения преступлений, в том числе, связанных с созданием, использованием и распространением вредоносных компьютерных программ.

Сдерживание кибервойн, противодействие проведению наступательных кибероперациий невозможны только технологическими (техническими) средствами и мероприятиями. Необходим *комплекс действий на политико-дипломатическом, правовом, технологическом и организационном направлениях*.

К *перспективным мероприятиям*[30] здесь, по мнению авторов, следует отнести:

- создание национальной системы защиты от вредоносных программ – элементов кибероружия (в первую очередь от программ нового поколения, рассматриваемых в настоящей работе) и методов их доставки[31];

- создание системы мониторинга и совместного реагирования на возникающие угрозы в области МИБ, где одним из базовых направлений деятельности должно стать отражение деструктивных информационных воздействий, исходящих как от государств, так и от террористических и криминальных структур[32];
- создание технических средств контроля за соблюдением норм международного права для киберпространства[33];
- создание системы глобального мониторинга всех событий, составляющих юридические факты злонамеренного использования ИКТ;
- создание единой системы регистрации фактов угрозы силой или ее применения, а также вооруженного нападения посредством злонамеренного использования ИКТ;
- разработка под эгидой международных организаций норм международного права применительно к киберпространству, а также адаптация действующих норм к условиям злонамеренного использования ИКТ в военных целях[34].

Проведение всех этих мероприятий в полной мере и в первую очередь является прямой и первостепенной обязанностью международных организаций, государств и национальных правительств. И России, и ее партнерам здесь по-прежнему принадлежит инициатива по разработке новых подходов миротворческого характера в киберпространстве.

В то же время становится все более очевидным тот факт, что сегодня ни одно государство неспособно в одиночку успешно противостоять современным угрозам, исходящим из киберпространства. Для решения этой проблемы особую значимость приобретают согласованная деятельность заинтересованных стран в области МИБ, превращение системы МИБ в еще одно средство разрешения межгосударственных противоречий.

Перечисленные выше мероприятия должны реализовываться в рамках государственной системы информационной безопасности Российской Федерации, а большая часть из них – одновременно и в рамках создаваемой системы МИБ.

Система МИБ, ее эффективное и своевременное формирование и укрепление позволят всем участникам процессов, протекающих в киберпространстве, в первую очередь государствам и их правительствам, создать надежную и защищенную среду, которая будет способствовать поддержанию международного мира и безопасности, включая мирное урегулирование споров и конфликтов, неприменение силы, невмешательство во внутренние дела, соблюдение основных прав и свобод человека.

Заключение

В современном киберпространстве возникают все новые и новые виды противоправных действий и риски для его акторов. Наибольшую опасность представляют *действия военно-политического характера*, которые проявляются в использовании ИКТ для достижения политических, экономических, военных целей посредством враждебного использования этих технологий (*боевые*, *диверсионные*, *разведывательные кибероперации и кибервойны*).

Эти угрозы, так или иначе связанные с *ведением войн и проведением специальных операций в киберпространстве, потенциально могут привести к нарушению международного мира и безопасности, к подрыву доверия в международных отношениях, способны отрицательно воздействовать на целостность и устойчивость функционирования критически важных инфраструктур*.

Защита таких инфраструктур должна осуществляться как на национальном уровне, так и в рамках системы МИБ, созданию которой наша страна уделяет особое внимание и прилагает большие усилия по продвижению соответствующих инициатив[35,36,37] на этом направлении.

Современная система МИБ, отвечающая угрозам и вызовам XXI в., позволит создать достаточные международные гарантии в области обеспечения безопасности использования современных ИКТ, осуществления членами международного сообщества согласованных и объективно обусловленных действий *по пресечению использования этих технологий для нанесения ущерба международному миру и безопасности как сейчас, так и в долгосрочной перспективе*.

Примечания

1 Начиная с 2009 г. Хотя есть данные, что программа Stuxnet была разработана еще в 2005–2006 гг.

2 Авторы намеренно опускают такие события последнего времени, как атаки хакеров (хактивистов) на эстонские и грузинские сайты в 2008 г., «цифровая и социальная арабская весна» 2011 г., обнародование секретной информации ресурсом WikiLeaks и Э. Сноуденом в 2010–2013 гг., которые некоторые специалисты относят к кибервойнам.

3 Исследовательский проект «Вредоносные программы нового поколения: источники разработки, цели, характер, особенности и последствия их применения» (I, II этапы), ИПИБ МГУ имени М.В. Ломоносова, ИИНТБ РГГУ,

октябрь 2014 г. [Электронный ресурс]. URL: http://www.iisi.msu.ru/articles/; http://iintb.rsuh.ru/science/student-projects.php (дата обращения: 07.01.2015).

4 *Марков А.С., Фадин А.А.* Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2014. № 1 (1). С. 28–36.

5 *Барри Ч.* Вызовы защиты критически важной инфраструктуры: надежность систем в цифровой век // Сб. тр. Восьмого междунар. форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», 21–24 апр. 2014 г., Гармиш-Партенкирхен, Германия. М.: Изд-во Моск. ун-та, 2014. С. 25–39.

6 Возможно, АЭС в Бушере.

7 Несмотря на всю сложность терминологической полемики вокруг понятия «кибервойна», авторы посчитали уместным воспользоваться термином из двуязычного англо-русского глоссария по кибербезопасности ИПИБ МГУ – Институт «Восток-Запад»: *Rauscher K.F., Yaschenko V.* The Russia-U.S. Bilateral on Cybersecurity. Critical Terminology Foundations / Karl Frederick Rauscher, Valery Yaschenko; EastWest Inst.; Information Security Inst. of Moscow State Univ. 2011. April. Iss. 1.

8 См. аргументы в статье: *Казарин О.В., Сальников А.А., Шаряпов Р.А., Ященко В.В.* Новые акторы и безопасность в киберпространстве // Вестник Московского университета. Серия 12: Политические науки. 2010. № 2. С. 71–84; № 3. С. 90–103.

9 Перечисленные выше вредоносные программы могут распространяться не только через сети, но и агентурным путем, например через флэш-носители. Прием / передача / накопление шпионской информации, внедрение вредоносных программ может осуществляться через заранее внедренные программно-аппаратные закладки и трансиверы, встраиваемые в USB-, WiFi-устройства, другое периферийное оборудование, подключаемое к компьютеру – объекту атаки. При этом атакуемые компьютеры могут быть физически отсоединены от сетей.

10 Может, здесь стоит ожидать только военного и / или политического эффекта (но не экономического)?

11 Как законодательно закрепленных, так и нет, опубликованных или секретных.

12 *Казарин О.В., Тарасов А.А.* Современные концепции кибербезопасности ведущих зарубежных государств // Вестник РГГУ. 2013. № 15. Сер. Информатика. Защита информации. Математика. С. 58–74.

13 Международная стратегия для киберпространства США. Процветание, безопасность и открытость сетевого мира, Белый дом, Вашингтон, май 2011 года (International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World) [Электронный ресурс] // Инофорум. URL: http://www.inoforum.ru/inostrannaya_pressa/mezhdunarodnaya_strategiya_po_dejstviyam_v_kiberprostranstve (дата обращения: 07.01.2015).

[14] DoD Strategy for Operating in Cyberspace (DSOC) [Электронный ресурс] // U.S. Department of Defense. URL: http://www.defense.gov/news/d20110714cyber.pdf (дата обращения: 07.01.2015).

[15] Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation [Электронный ресурс] // North Atlantic Treaty Organization. URL: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (дата обращения: 07.01.2015).

[16] То есть здесь речь уже не идет о применении конвенциональных ответных военных действий.

[17] Есть еще ряд американских документов, в которых боевые действия в киберпространстве определены как фактор, повышающий боевой потенциал США в операциях объединенных сил. Это положение было закреплено в наставлении Объединенного штаба Комитета начальников штабов Вооруженных сил США (ОШ КНШ ВС США) JP 3-13, 2006, а 27 ноября 2012 г. уточнены в новой редакции JP 3-13. По сути, эти документы в юридическом аспекте зафиксировали создание единой системы и общей для всех видов ВС США военной стратегии ведения боевых действий в киберпространстве, дополняющей и равнозначной другим сферам ведения боевых действий. В сентябре 2012 г. председатель ОШ КНШ ВС США генерал Мартин Демпси издал директиву «Единые силы – 2020», излагающую основополагающие концепции ведения совместных операций, которая значительно повысила значение информационных операций в сражениях XXI в., делая упор на глобальные интегрированные операции, основой которых станут «проводимые одновременно или отдельно от сил общего назначения операции сил специальных операций и кибероперацийВС США».

[18] National Defense Authorization Act for Fiscal Year 2014 [Электронный ресурс] // The Library of Congress. URL: http://thomas.loc.gov/cgi-bin/query/z?c113:H.R.3304 (дата обращения: 07.01.2015).

[19] Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation [Электронный ресурс].

[20] Статья о самообороне.

[21] Североатлантический договор. Вашингтон, Федеральный округ Колумбия, 4 апреля 1949 г. [Электронный ресурс] // Организация Североатлантического Договора. URL: http://www.nato.int/cps/ru/natohq/official_texts_17120.htm (дата обращения: 07.01.2015).

[22] Заявление по итогам встречи на высшем уровне в Уэльсе, обнародовано главами государств и правительств, участвующими в заседании Североатлантического союза в Уэльсе 4–5 сентября 2014 года [Электронный ресурс] // Организация Североатлантического Договора. URL: http://www.nato.int/cps/ru/natohq/official_texts_112964.htm (дата обращения: 07.01.2015).

[23] LÜKEX (аббрев.) – система учений в ФРГ на национальном уровне (с участием земель) по урегулированию кризисных ситуаций при стихийных бед-

ствиях, технологических катастрофах, террористических угрозах, эпидемиях и других чрезвычайных ситуациях.

24 *Казарин О.В., Сальников А.А., Шаряпов Р.А., Ященко В.В.* Указ. соч.

25 *Горбачев Ю.* Кибервойна уже идет. Армия втягивается в информационное противоборство // Независимое военное обозрение. 2013. 12 апр.

26 Выступление Президента РФ В.В. Путина на заседании Совета Безопасности 1 октября 2014 года, Москва, Кремль [Электронный ресурс] // Президент России. URL: http://www.kremlin.ru/transcripts/46709 (дата обращения: 07.01.2015).

27 Современное состояние и перспективы развития военного сотрудничества Российской Федерации в области международной информационной безопасности: Сб. мат-лов / Под общ. ред. С.А. Комова. М.: Мин-во обороны РФ, 2014. 151 с.

28 Международная информационная безопасность: проблемы и решения / Под общ. ред. С.А. Комова. М., 2011.

29 Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [Электронный ресурс] // Информационно-правовой портал «Гарант.ру». URL: http://www.garant.ru/products/ipo/prime/doc/70541072/ (дата обращения: 07.01.2015).

30 Данные мероприятия могут пересекаться, дополнять друг друга или объединяться в различные пулы.

31 Создаваемой, например, в рамках национальной системы противодействия кибератакам.

32 Современное состояние и перспективы развития военного сотрудничества...

33 *Пилюгин П.Л.* Проблемы создания технических средств контроля за соблюдением разрабатываемых норм международного права для киберпространства // Сб. тр. Восьмого междунар. форума... С. 122–133.

34 *Стрельцов А.А.* Основные направления развития международного права вооруженных конфликтов применительно к киберпространству // Там же. С. 52–61.

35 Одна из последних успешных инициатив России: Резолюция, принятая Генеральной Ассамблеей ООН 2 декабря 2014 г., A/RES/69/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс] // Организация Объединенных Наций. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/662/43/PDF/N1466243.pdf?OpenElement (дата обращения: 07.01.2015).

36 Конвенция об обеспечении международной информационной безопасности (концепция) [Электронный ресурс] // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 07.01.2015).

37 О Европейском Альпбахском форуме «В поисках определенности и безопасности» 12–31 августа 2013 г., Альпбах, Австрия [Электронный ресурс] // Институт проблем информационной безопасности МГУ имени М.В. Ломоносова. URL: http://www.iisi.msu.ru/news/news74 (дата обращения: 07.01.2015).

В.А. Конявский, И.Г. Назаров
С.Т. Петров, А.А. Тарасов

ФОРМИРОВАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ КУЛЬТУРЫ

В статье рассматривается комплексный подход к обеспечению информационной безопасности в сфере культуры. На основе анализа предметной области и обследования учреждений культуры выявлены основные проблемы и трудности при разработке системы информационной безопасности. Представлены концепция информационной безопасности, методики оценки информационных активов, рисков и угроз, другие методики, комплект политик информационной безопасности, дорожная карта. В предлагаемом комплексе документов впервые освещены основные концептуальные и практические подходы к построению системы информационной безопасности как сферы культуры в целом, так и отдельных учреждений культуры.

Ключевые слова: культура, культурные ценности, информационная безопасность, информационные активы, риски и угрозы.

Введение

Культурная политика признана неотъемлемой частью стратегии национальной безопасности Российской Федерации[1]. Важность проблем обеспечения информационной безопасности в сфере культуры давно уже признана на государственном уровне, что отражено, в частности, в концептуальном документе – Доктрине информационной безопасности Российской Федерации[2]. Вместе с тем в одном из самых исчерпывающих списков угроз национальной безопасности Российской Федерации угрозы культуре не упомянуты вообще[3], а проблемы информационной безопасности в сфере культуры не фигурируют даже в 300-страничном проекте Закона о культуре.

Важнейшими причинами такого противоречивого положения дел, на наш взгляд, являются, в том числе, следующие:

– сфера культуры является обширной, всепроникающей и трудноочерчиваемой областью деятельности как с философско-содержательной, так и с прагматической точки зрения, например законодательной;
– вопросы информационной безопасности культуры находятся на своеобразной «нейтральной полосе» между гуманитарными и техническими проблемами;
– в сфере культуры остается низким уровень информатизации, компьютерной грамотности и культуры информационной безопасности.

Попыткой начать разрешение сложной ситуации с информационной безопасностью в культуре стала постановка Минкультуры России НИР «Анализ базовых условий и формирование инструментария построения системы обеспечения информационной безопасности в сфере культуры» (открытый аукцион № 0173100007713001485). Результатом НИР стал разработанный авторами в 2013–2014 гг. комплекс документов:

Концепция информационной безопасности;

Методика оценки информационных активов;

Модели угроз и рисков информационной безопасности;

Методики оценки угроз и рисков информационной безопасности;

Методика оценки уязвимостей информационных систем (ресурсов);

Меры обеспечения информационной безопасности информационных систем (ресурсов);

Методика оценки эффективности системы обеспечения информационной безопасности;

Комплект политик информационной безопасности;

Дорожная карта реализации мероприятий по обеспечению информационной безопасности.

При их подготовке было проведено изучение предметной области, включающее анализ нормативно-правовой базы обеспечения информационной безопасности, анализ существующих информационных систем и ресурсов в сфере культуры, а также выявление основных информационных потребностей, влияющих на обеспечение информационной безопасности.

Ниже рассмотрены вопросы построения системы обеспечения информационной безопасности в сфере культуры с учетом полученных в НИР результатов, появления ряда новых документов, таких как «Основы государственной культурной политики», про-

ект «Закона о культуре»[4], и начала подготовки новой редакции Доктрины информационной безопасности.

Условия формирования и основные проблемы информационной безопасности в сфере культуры

В условиях стремительного развития информационно-коммуникационных технологий (ИКТ) в России достаточно высокими темпами происходит формирование и повсеместное распространение культурных ценностей, представленных в цифровой форме. Миллионы архивных документов и каталожных карточек, сотни тысяч изданий и музейных экспонатов, десятки тысяч фонограмм и фильмов уже представлены в цифровом виде и многие из них размещены на тысячах сайтах, в разнообразных базах данных. Некоторые проекты в области цифрового наследия культуры масштабны и уникальны, демонстрируют высокий уровень научной проработки и программно-технических решений, представляют собой шедевры дизайна. Государственной программой Российской Федерации «Информационное общество (2011–2020 годы)» предусмотрено создание огромных массивов архивной, библиотечной и музейной информации в цифровой форме. Тем не менее в сфере культуры отсутствуют механизмы гарантии целостности, доступности и, при необходимости, конфиденциальности имеющихся и вновь создаваемых информационных активов.

Формирование, использование и защита информационных активов затруднены по ряду причин, включая низкий уровень информатизации отрасли, слабую проработку нормативно-правовой базы, отсутствие элементарных навыков информационной безопасности. Одна из основных причин множества нерешенных проблем в этой области связана с отсутствием системы управления и принятия решений по информатизации и информационной безопасности культуры на всех уровнях: от лиц, отвечающих за государственную культурную и информационную политику, до директора краеведческого музея.

Культурная политика – чрезвычайно широкая и в значительной мере неопределенная предметная область, которая охватывает такие сферы государственной и общественной жизни, как «все виды культурной деятельности, гуманитарные науки, образование, межнациональные отношения, поддержка русской культуры за рубежом, международное гуманитарное и культурное сотрудничество, а также воспитание и самовоспитание граждан, просвещение,

развитие детского и молодежного движения, формирование информационного пространства страны»[5].

Разнообразны и многочисленны объекты информационных угроз, к которым потенциально относятся и все культурные ценности, а именно нравственные и эстетические идеалы, нормы и образцы поведения, языки, диалекты и говоры, национальные традиции и обычаи, исторические топонимы, фольклор, художественные промыслы и ремесла, произведения культуры и искусства, результаты и методы научных исследований культурной деятельности, имеющие историко-культурную значимость здания, сооружения, предметы и технологии, уникальные в историко-культурном отношении территории и объекты. Большинство имеющихся угроз не идентифицированы и не ранжированы.

Один из основных объектов угроз – информационные активы не инвентаризированы и не проведена их оценка, в том числе в силу отсутствия соответствующих методик.

Перманентно возникают новые, быстроменяющиеся и зачастую трудноидентифицируемые угрозы национальной культуре, связанные с процессами глобализации и массового распространения ИКТ.

Многие объекты культуры уникальны, в том числе в силу этого чрезвычайно трудно оценить соответствующие информационные риски и возможный ущерб. Серьезной проблемой являются риски информационной безопасности, имеющие организационный характер. Зачастую не определены зоны информационной ответственности организаций, отвечающих за целые сегменты культурной деятельности. Практически у всех учреждений культуры отсутствуют политики информационной безопасности.

Для формулировки и закрепления целей, задач, принципов и основных направлений информационной безопасности культуры Российской Федерации в области формирования, использования и совершенствования информационных активов и информационной инфраструктуры культуры для развития в России информационного общества на основе традиционных культурных ценностей и с учетом особенностей пройденного исторического пути был подготовлен проект концептуального документа.

При подготовке документа учитывался большой комплекс источников в области культуры, информационных технологий и безопасности. Особо следует отметить Хартию Юнеско о сохранении цифрового наследия, Стратегию развития информационного общества в Российской Федерации, Доктрину информационной безопасности Российской Федерации.

Проект Концепции информационной безопасности Российской Федерации в сфере культуры

Основной целью обеспечения информационной безопасности Российской Федерации в сфере культуры является предотвращение (минимизация) ущерба культуре в результате деструктивных воздействий на информацию и информационную инфраструктуру, могущих привести к нарушению достоверности, аутентичности, конфиденциальности, доступности и целостности информации, связанной с культурными ценностями и деятельностью в сфере культуры.

Концепция является базовым документом по созданию и развитию системы обеспечения информационной безопасности Российской Федерации в сфере культуры и предназначена для использования в практической деятельности должностных лиц, ответственных за создание, использование и развитие информационных активов и инфраструктуры в сфере культуры, представителей проектных и сервисных организаций по обеспечению требуемого уровня защищенности информации и инфраструктуры в сфере культуры, а также участников информационного взаимодействия в сфере культуры, по соблюдению ими установленных требований информационной безопасности.

Концепция имеет следующую структуру:

общие положения и основные понятия,

проблемная ситуация,

цели и задачи обеспечения информационной безопасности,

принципы обеспечения и построения системы информационной безопасности,

субъекты информационной безопасности,

объекты информационной безопасности,

обеспечение информационной безопасности.

Основное содержание обеспечения информационной безопасности в сфере культуры состоит в поддержании правовых, информационных, социокультурных и институциональных механизмов, а также ресурсных возможностей государства и общества на уровне, отвечающем национальным интересам Российской Федерации в сфере обеспечения безопасности культуры и информации.

Состояние информационной безопасности в сфере культуры зависит от духовного, культурного, научно-технического и экономического потенциала страны, а также эффективности функционирования системы обеспечения информационной безопасности как части системы национальной безопасности.

Стратегическими целями информационной безопасности в сфере культуры являются:

обеспечение безопасности информационных активов как части культурного наследия;

недопущение несанкционированного использования информации, влияющей на безопасность культурного наследия;

обеспечение информационной безопасности сферы культуры как отрасли.

Долгосрочными целями информационной безопасности в сфере культуры являются:

обеспечение гарантированного сохранения и доступа к информации, представляющей в полноте и целостности культурные ценности Российской Федерации;

обеспечение защищенности информации и инфраструктуры, связанной с охраной культурных ценностей Российской Федерации, а также информации, связанной с обеспечением прав на результаты интеллектуальной деятельности и персональные данные;

формирование доверенной информационной среды как основы единого цифрового культурно-исторического пространства Российской Федерации;

обеспечение всеобщей доступности цифрового наследия;

обеспечение непрерывности управления в сфере культуры и непрерывности функционирования учреждений культуры в информационной сфере.

Субъектами отношений в области информационной безопасности культуры, а также носителями и выразителями интересов в этой области являются:

народ России;

этнические и культурные сообщества;

граждане России;

Российская Федерация и ее регионы;

Министерство культуры Российской Федерации;

органы федеральной, региональной и муниципальной власти;

учреждения культуры различной ведомственной подчиненности и форм собственности;

юридические лица, действующие в сфере культуры и информации;

деятели культуры и работники сферы культуры;

международное сообщество и граждане иностранных государств;

интеллектуальные информационные системы.

Концепции, стандарты и иные документы в области информационной безопасности разрабатываются, как правило, в контексте

организации. Такой подход может быть адаптирован и применен к учреждениям культуры и органам управления культурой. Однако значительная и значимая часть культурных ценностей (например, язык, обычаи, верования) заведомо не укладывается в масштаб какой-либо организации и даже в государственные и национальные рамки.

Это выдвигает перед обеспечением информационной безопасности в сфере культуры весьма сложные и малоисследованные задачи, существенно расширяет круг субъектов и их интересов по сравнению с традиционно рассматриваемыми субъектами и интересами в области информационной безопасности.

В Концепции выделены основные национальные интересы по обеспечению информационной безопасности в сфере культуры. Эти интересы заключаются:

в развитии информационной составляющей обеспечения духовного единства российского общества, основанного на культурных и исторических традициях;

в развитии и защите прав и свобод граждан в области культуры и информации, пользовании учреждениями культуры, доступа к культурным ценностям;

в увеличении защищенности российской культуры от деструктивных воздействий, прежде всего информационного характера;

в уменьшении регионального, социального и профессионального информационного неравенства в сфере культуры;

в вовлечении граждан в обеспечение сохранности исторического и культурного наследия, наращивания информационного потенциала культуры;

в обеспечении полноты, сохранности и доступности цифрового культурного наследия Российской Федерации;

в превращении российской культуры в мировой ресурс развития глобального информационного общества.

В силу ограниченности объема статьи мы не рассматриваем здесь интересы иного масштаба и иных субъектов.

Объектом информационной безопасности в сфере культуры является объект с присущими ему свойствами, обусловленными информацией или информационной инфраструктурой, связанными с деятельностью в сфере культуры. Национальные и иные интересы в информационной области сферы культуры являются объектом информационной безопасности.

К числу важнейших объектов обеспечения информационной безопасности Российской Федерации в сфере культуры относятся:

русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения

народов – государств-участников Содружества Независимых Государств;

языки, нравственные ценности, культурное наследие народов и народностей Российской Федерации;

объекты интеллектуальной собственности.

Основными типами объектов информационной безопасности в сфере культуры являются:

информационные активы;

информационная инфраструктура;

информационные процессы, связанные с осуществлением деятельности в сфере культуры;

культурные ценности, другие объекты культуры;

субъекты информационной деятельности, связанные со сферой культуры.

Информационные активы включают:

цифровые образы объектов культуры;

метаданные культурных ценностей;

учетную информацию по культурным ценностям;

справочную информацию по культурным ценностям;

нормативно-правовую и управленческую документацию и сообщения;

персональные данные;

иную информацию в сфере культуры, представляющую ценность для государства, общества или граждан.

Информационные активы могут иметь цифровую и аналоговую форму, относиться к материальной или нематериальной части культурного наследия. Основными объектами информационной защиты в целях настоящей Концепции являются цифровые информационные активы, представляющие культурные ценности.

Информационные активы должны быть идентифицированы, описаны и инвентаризированы. Информационные активы сферы культуры могут включаться в реестр государственных (региональных, муниципальных) информационных ресурсов.

Для целей настоящей Концепции наиболее важными свойствами информационной безопасности активов являются их доступность и сохранность. Описание информационных активов, подлежащих защите, должно находиться в специальных реестрах.

Основными *угрозами информационной безопасности* Российской Федерации в сфере культуры являются:

низкие темпы формирования качественных информационных ресурсов и развития информационной инфраструктуры в сфере

культуры, проходящие без учета требований информационной безопасности;

непреднамеренные неблагоприятные воздействия на информацию и элементы информационной инфраструктуры;

массовое деструктивное информационное воздействие на традиционные культурные ценности;

противоправное использование информации, связанной с обеспечением безопасности культурных ценностей и объектов культуры;

неправомерное распространение информации, затрагивающей интересы граждан и правообладателей.

Видами угроз информационной безопасности Российской Федерации в сфере культуры являются:

дезорганизация и разрушение системы информационного обеспечения накопления и сохранения культурных ценностей;

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной культурной политики Российской Федерации.

Целью обеспечения информационной безопасности является защита интересов субъектов информационных отношений, возникающих при функционировании информационных систем. Данная цель достигается посредством:

соблюдения установленного порядка использования, полноты, целостности, достоверности информации;

предотвращения утечки, хищения, утраты информации, а также неправомерных действий по ее уничтожению, модификации, искажению, несанкционированному копированию, блокированию; предотвращения других форм незаконного вмешательства в функционирование информационных систем;

сохранности информации конфиденциального характера в соответствии с действующим законодательством Российской Федерации, нормативными правовыми актами и методическими документами в области обеспечения информационной безопасности;

соблюдения прав пользователей в соответствии с их полномочиями (ролями) по доступу к информационным процессам, технологиям, сервисам и средствам их обеспечения в информационных системах;

сохранения возможности управления процессом обработки и пользования информацией;

обучения обслуживающего персонала информационных систем правилам безопасной работы с комплексом программно-технических средств системы.

Обеспечение информационной безопасности включает совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов от угроз безопасности. Экономический эффект от реализации этих мер проявляется в снижении величины возможного материального, морального и иных видов ущерба.

В дальнейшем при подготовке перспективных документов по информационной безопасности культуры следует, на наш взгляд, проводить структуризацию интересов, объектов, угроз, рисков и др. по группам, связанным с информационным потенциалом, информационным пространством, а также правами и обязанностями в сфере культуры.

Проекты методик и иных документов по обеспечению информационной безопасности в сфере культуры

Предлагаемые материалы опираются на международные, национальные и отраслевые стандарты, включая семейство стандартов менеджмента информационной безопасности ГОСТ Р ИСО/МЭК 27000, методические и нормативные документы ФСТЭК и ФСБ в области информационной безопасности[6], ряд иных действующих и разрабатываемых документов. В представленных методиках нашли отражение международные и национальные методические, инструктивные, научно-исследовательские и иные материалы в области организации архивного, библиотечного и музейного дела, а также цифрового наследия. В данных документах реализуется применение риск-ориентированного подхода к обеспечению информационной безопасности в сфере культуры.

Для принятия решений в области развития культуры, ее информатизации, обеспечения информационной безопасности необходима оценка значимости информационных активов в сфере культуры. Инвентаризация и оценка информационных активов и систем является отправной точкой для оценки угроз и рисков.

Оценка (историческая, стоимостная, иная) культурных ценностей в целом и оценка значимости информационных активов в частности являются сложными процессами, зависящими от множества факторов: культурно-исторических, религиозных, идеологических, социально-экономических, финансовых и иных[7].

Оценка значимости информационного актива представляет собой совокупную оценку объекта культуры и цифрового объекта. Спектр информационных активов сферы культуры чрезвычайно широк: от оцифрованной рукописи до репутации учреждения культуры. В связи с этим создание какой-либо типовой методики оценки информационных активов сферы культуры весьма проблематично, хотя, очевидно, возможна общая структура методики для оценки различных типов активов.

В документе *«Методика оценки информационных активов»* приведена такая общая структура. К структурным элементам методики относятся показатели и критерии значимости информационных активов; оценка сферы применения; оценка значимости информационных систем и активов на различных этапах их жизненного цикла; вывод из оборота, ликвидация активов; корректировка оценки.

Схемы оценки и уровни значимости информационных активов и систем в сфере культуры включают схемы оценки объектов цифрового наследия и их портфелей (собраний, коллекций), оценки значимости информационно-поисковых систем, а также оценку значимости веб-сайтов.

На данную методику можно опираться при выборе процедур оценки разнородных информационных активов, представляющих различные типы культурных ценностей и являющихся результатом различных видов культурной деятельности. Примеры оценки разнородных активов с помощью метода анализа иерархий приведены нами ранее[8,9].

Комплексный анализ объектов, угроз и рисков представлен в документе *«Модели угроз и рисков информационной безопасности»*.

Основными типами объектов информационной безопасности в сфере культуры являются:

информационные активы;

информационная инфраструктура и ее элементы;

информационные процессы, связанные с осуществлением деятельности в сфере культуры;

культурные ценности, другие объекты культуры;

субъекты информационной деятельности, связанные со сферой культуры.

Основными угрозами информационной безопасности Российской Федерации в сфере культуры являются:

низкие темпы формирования качественных информационных ресурсов и развития информационной инфраструктуры в сфере культуры, проходящие без учета требований информационной безопасности;

непреднамеренные неблагоприятные воздействия на информацию и элементы информационной инфраструктуры;

массовое деструктивное информационное воздействие на традиционные культурные ценности;

противоправное использование информации, связанной с обеспечением безопасности культурных ценностей и объектов культуры;

неправомерное распространение информации, затрагивающей интересы граждан и правообладателей.

Видами угроз информационной безопасности Российской Федерации в сфере культуры являются:

дезорганизация и разрушение системы информационного обеспечения накопления и сохранения культурных ценностей, включая архивы;

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики Российской Федерации.

В *«Методике оценки угроз и рисков информационной безопасности»* представлены оценки угроз и рисков объектам информационной безопасности в сфере культуры, проведенные на основе собственного ранжирования угроз и рисков с применением апробированных методик, применяемых в различных сферах и областях, таких как банковская деятельность[10] и защита персональных данных[11].

Представлен перечень классов основных источников угроз информационной безопасности, их описание и возможный ущерб, приведены классы защищенности информационных систем и методики оценки угроз и рисков.

Для эффективной защиты информационных активов в сфере культуры необходимы удобные средства и методы постоянной и оперативной корректировки политики безопасности с учетом изменения характера угроз, возникновения новых угроз, изменений в конфигурации информационных систем, статистики эксплуатации и др.

Кроме того, следует оценивать адекватность применяемых и планируемых мер защиты, из возможных (в том числе вновь появляющихся) мер защиты необходимо оперативно выбирать наиболее эффективные (в том числе экономически).

Представляемая методика должна обеспечить решение следующих задач:

документирование угроз;

сравнительная оценка угроз (для определения уязвимостей информационных активов и первоочередных направлений защиты);

абсолютная оценка угроз в терминах ожидаемого материального ущерба от их реализации;

оценка эффективности и экономического обоснования мер защиты;

возможность проведения анализа вида «что, если...».

Предлагаемая ниже методика рассматривает практически применимый вариант решения всех перечисленных задач в некотором разумном приближении.

Основные объекты угроз, в частности информационные активы и элементы инфраструктуры, а также существенные характеристики этих угроз были рассмотрены нами выше.

В методике содержатся:

сценарии реализации угроз и упрощенное матричное описание;

оценка вероятности неумышленных начальных угроз;

оценка вероятности умышленных начальных угроз;

технико-экономическое обоснование мер защиты;

порядок (алгоритм) проведения оценки угроз;

схема анализа рисков;

алгоритм оценки рисков с помощью метода анализа иерархий.

Разработанная *«Методика оценки уязвимостей информационных систем (ресурсов) в сфере культуры»* применима для оценки уязвимостей, позволяющих реализовать следующие основные деструктивные действия:

уничтожение программными средствами или физическим воздействием;

модификация информации;

хищение носителя информации;

блокирование информации;

копирование информации.

Настоящая методика является модельной и на ее основе должны разрабатываться частные методики оценки уязвимостей конкретных информационных систем (ресурсов) Минкультуры России и подведомственных учреждений.

Уязвимости присущи следующим видам активов:

физическое окружение;

персонал, процедуры управления, администрирования и механизмы контроля;

процессы деятельности и получаемые услуги;

технические средства, программное обеспечение, телекоммуникационное оборудование;

информационные ресурсы.

Методика включает общий порядок оценки, идентификацию уязвимостей, оценивание уязвимостей. Для целей идентификации все существующие уязвимости делятся на две группы: технические и организационные.

Для идентификации технических уязвимостей проводятся следующие мероприятия по анализу защищенности:

ручные проверки системной конфигурации;

сетевое и хостовое сканирование;

тестовые испытания;

тесты на проникновение;

анализ программных кодов.

Организационные уязвимости обычно заключаются в отсутствии или неправильном применении механизмов контроля. Поэтому основным источником идентификации организационных уязвимостей служат документы, содержащие лучшие мировые практики в области обеспечения информационной безопасности, например семейство стандартов ISO/IEC 27000.

Для оценки уязвимостей необходимо идентифицировать существующие механизмы обеспечения информационной безопасности и оценить, насколько они результативны. Уязвимости в данной методике оцениваются по трехуровневой качественной шкале. Значение уровня уязвимости показывает, насколько вероятно успешное осуществление угрозы с использованием данной уязвимости в случае, если эта угроза будет реализовываться.

Документ *«Меры обеспечения информационной безопасности информационных систем (ресурсов)»* детализирует организационные и технические меры защиты информации. Методический документ предназначен для формирования мер обеспечения информационной безопасности для конкретных информационных систем (ресурсов) в сфере культуры на основе оценок угроз, рисков и уязвимостей.

Выбор мер защиты информации для их реализации в информационной системе осуществляется в ходе проектирования системы защиты информации в соответствии с техническим заданием на создание информационной системы и техническим заданием на создание системы защиты информации информационной системы.

Меры защиты информации выбираются исходя из класса защищенности информационной системы, определяющего требуемый уровень защищенности содержащейся в ней информации, и угроз

безопасности информации, включенных в модель угроз безопасности информационной системы, а также с учетом структурно-функциональных характеристик информационной системы, к которым относятся структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, взаимосвязи с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности функционирования системы.

Правила и процедуры по реализации требований о защите информации и мер защиты информации в конкретной информационной системе определяются в эксплуатационной документации на систему защиты информации и организационно-распорядительных документах по защите информации.

В информационной системе подлежат реализации следующие меры защиты информации:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита носителей информации;

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности информации;

обеспечение целостности информационной системы и информации;

обеспечение доступности информации;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств и систем связи и передачи данных.

«Методика оценки эффективности системы обеспечения информационной безопасности» предназначена для оценки эффективности применения совокупности мер и средств технической защиты информации на типовых объектах информатизации как от отдельной угрозы, так и от заданной совокупности антропогенных и техногенных угроз.

В методике используется основной показатель степени защищенности информации, показывающий, насколько ущерб от реализации

заданной совокупности угроз безопасности информации меньше неприемлемого уровня. Производные (сравнительные) показатели являются вспомогательными и рассчитываются на основе показателя «степень защищенности информации», определенного для условий отсутствия и применения оцениваемых мер и средств защиты.

Общий алгоритм расчета показателей основан на следующих допущениях:

перечень и характеристики возможных угроз заданы или установлены до проведения расчетов;

техногенные угрозы безопасности информации на объекте информатизации имеются всегда;

угрозы могут быть реализованы независимо друг от друга;

ущерб от реализации совокупности угроз аддитивен относительно ущерба, наносимого в результате выполнения разных деструктивных действий при реализации одной или разных угроз;

если одно и то же деструктивное действие может выполняться при реализации разных угроз, то ущерб от его выполнения не суммируется по угрозам;

опасность деструктивного действия оценивается применительно к самой важной информации, конфиденциальность, целостность или доступность которой нарушается при выполнении данного деструктивного действия;

влияние мер и средств технической защиты информации на эффективность защиты информации взаимонезависимо.

В методике приведены алгоритмы определения коэффициентов опасности деструктивных действий, выявления состава возможных угроз безопасности информации, определения состава деструктивных действий, которые могут быть выполнены при реализации угроз, оценки коэффициентов опасности деструктивных действий. Также рассмотрен порядок: определения вероятностей реализации угроз безопасности информации и выполнения деструктивных действий; учета мер и средств технической защиты информации при оценке опасности угроз; учета влияния мер и средств технической защиты информации на вероятность реализации угроз; учета влияния мер и средств технической защиты информации на коэффициенты опасности угроз. Для реализации алгоритмов приводится перечень необходимых исходных данных, порядок их подготовки и проведения расчетов по методике.

В приложениях к методике приведены необходимые формы анкет и примеры, связанные с ее использованием.

Политика информационной безопасности призвана донести в сжатом виде до сотрудников, посетителей и партнеров учреждения

культуры цели, задачи и защитные меры как по информационной безопасности в целом, так и по ее отдельным аспектам[12].

«Комплект политик информационной безопасности в сфере культуры» включает на данный момент следующие документы:

модельная политика информационной безопасности учреждения культуры;

политика инвентаризации информационных активов в сфере культуры;

политика обеспечения целостности информационных активов в сфере культуры;

политика по обеспечению информационной безопасности при управлении доступом к информационным ресурсам;

политика обработки персональных данных;

политика по антивирусной защите;

политика мониторинга инцидентов информационной безопасности;

политика реализации системы обеспечения информационной безопасности.

Массовое использование информационных технологий в сфере культуры, специфика отдельных видов культурной деятельности потребуют формирования как общих, так и «специфических» политик в области информационных технологий и информационной безопасности. В частности, необходимы:

политика использования цифровой подписи;

политика безопасного применения облачных решений;

политика безопасности цифрового наследия Российской Федерации;

политика безопасности Государственного каталога Музейного фонда Российской Федерации;

политика безопасности единого читательского билета;

политика безопасности web-сайтов учреждений культуры.

В документе *«Дорожная карта реализации мероприятий по обеспечению информационной безопасности»* представлены общее описание «дорожной карты», система показателей и схема плана мероприятий до 2018 г. Предметом плана является система мер по обеспечению информационной безопасности культуры в целом, а также отдельных видов культурной деятельности и культурных ценностей. «Дорожной картой» предусматриваются:

включение мер по защите информации в приоритеты деятельности органов исполнительной власти и учреждений культуры;

разработка нормативно-правовой базы информационной безопасности в сфере культуры;

внедрение лучших практик и систем обеспечения информационной безопасности в деятельности Минкультуры России и подведомственных учреждений, субъектах Российской Федерации;

формирование цифровой доверенной среды культурно-исторического пространства России;

повышение доступности и сохранности культурного наследия за счет реализации мер по обеспечению информационной безопасности;

повышение культуры информационной безопасности граждан и организаций Российской Федерации.

Среди мероприятий Дорожной карты можно выделить разработку ведомственных стандартов информационной безопасности; создание программно-технического комплекса «Реестр защищенных информационных активов в сфере культуры»; создание прототипа ведомственной системы информационной безопасности; разработку распределенной системы долговременного хранения электронных документов.

Заключение

Разработка инструментария системы обеспечения информационной безопасности в сфере культуры является задачей, решение которой необходимо рассматривать в неразрывной связи с вопросами сохранения и доступности культурного наследия Российской Федерации.

Подготовленные документы должны позволить создать эффективную систему информационной безопасности в сфере культуры как часть системы сохранения культурного наследия народов Российской Федерации и являются неотъемлемой частью политики в области общенациональной и информационной безопасности, использования «мягкой силы» в международных отношениях, в развитии информационного общества.

В результате создания системы информационной безопасности на основе разрабатываемого инструментария:

увеличится сохранность и доступность культурных ценностей;

повысится упорядоченность и возрастет качество информационных систем и ресурсов;

возрастет защищенность информационных систем и ресурсов активов как части культурного наследия;

будут обеспечены меры информационной безопасности сферы культуры как отрасли.

Важными задачами следующих этапов являются подготовка комплекса документов в отдельных областях культурной деятель-

ности (архивное, музейное, библиотечное дело и др.); создание иерархий взаимоувязанных документов от национальной безопасности до учреждения культуры; увязка информационной безопасности с другими видами безопасности (разработка документов по комплексной безопасности в сфере культуры).

Примечания

[1] Основы государственной культурной политики [Электронный ресурс] // Президент России. URL: http://news.kremlin.ru/media/events/files/41d526a877638a8730eb.pdf (дата обращения: 09.01.2015).

[2] Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/5.html (дата обращения: 09.01.2015).

[3] *Кордонский С.Г.* Классификация и ранжирование угроз // Отечественные записки. 2013. № 2 (53). С. 52–73.

[4] Проект Закона о культуре в Российской Федерации [Электронный ресурс] // Министерство культуры России. URL: http://mkrf.ru/upload/mkrf/mkdocs2014/26_11_2014_1.docx (дата обращения: 09.01.2015).

[5] Основы государственной культурной политики [Электронный ресурс].

[6] См., например: Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 г. Москва «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

[7] *Шестаков В.А.* Комплексная концепция музейной безопасности. СПб.: АНО НИИ СМД, 2013. 199 с.

[8] *Петров С.Т., Тарасов А.А.* Обеспечение безопасности информационных активов в сфере культуры // Вестник МФЮА. 2014. № 3. С. 57–64.

[9] *Сорокин А.Д., Казарин О.В., Петров С.Т., Тарасов А.А.* Применение метода анализа иерархий в области сохранения цифрового наследия // Современные проблемы и задачи обеспечения информационной безопасности: Тр. Всеросс. науч.-практ. конф. «СИБ – 2014» / Отв. ред. О.А. Макарова. М., 2014. С. 67–73.

[10] *Зенкевич В., Шатов В.* Информационные риски: анализ и количественная оценка // Бухгалтерия и банки. 2007. № 1. С. 50–53.

[11] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена приказом ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] // ФСТЭК России. URL: http://fstec.ru/component/attachments/download/290 (дата обращения: 09.01.2015).

[12] *Коваленко Ю.И., Матюнин С.А.* Разработка политики информационной безопасности организации. М.: МИНИТ ФСБ России, 2013. 172 с.

А.А. Пестряев, Л.И. Воронова,
В.И. Воронов

ПРОЕКТИРОВАНИЕ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ ДЛЯ СБОРА ТЕКСТОВОЙ ИНФОРМАЦИИ ИЗ СЕТИ

В статье рассматривается проектирование мультиагентной системы МАС «Стоп-ТСН», которая занимается сбором ссылок из Интернета. Система разработана для поиска запрещенных слов и выражений на страницах социальных сетевых сервисов. Онтология содержит слова и выражения о суициде, наркотиках и терроризме.

Проведено проектирование агентов системы, баз данных, механизмов доступа в глобальную сеть, выбраны средства реализации проекта, осуществлена реализация МАССТИС «Стоп-ТСН». Проведено тестирование. На момент написания статьи система собрала более 10 000 ссылок на страницы, содержащие «опасную» информацию.

Проектируемая МАС учитывает многоядерность архитектуры компьютера, анализируя размер КЭШ-памяти и распределяя работу агентов на разные ядра процессора.

Работа выполнена с использованием комплекса современных информационных технологий, таких как «Qt Creator v. 4.7.4», «MSSQL Server 2012», «Boost C++ Libraries v.1.53».

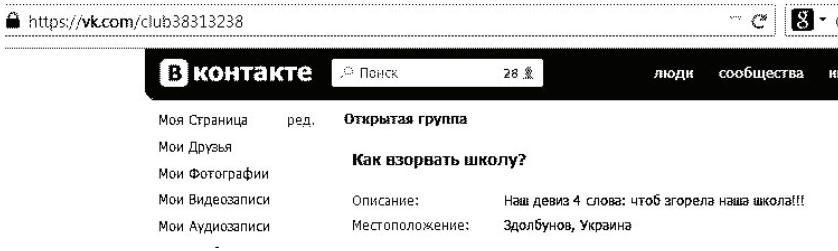
Преимущества разработанной системы по сравнению с существующими рассмотрены на конкретных примерах.

Ключевые слова: мультиагентная система, вредоносная информация, КЭШ-память, многоядерность компьютера, суицид, терроризм, наркотики.

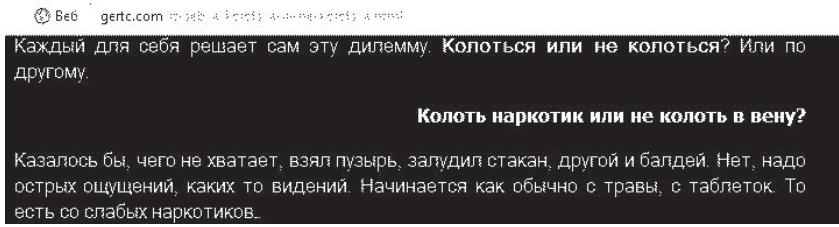
Введение

Сравнительно недавно, 20 лет назад, в жизни человека появился Интернет и за этот короткий промежуток времени занял в ней значимое место. Данные опроса фонда «ФОМнибус»[1] в 2013 г. показывают, что люди используют Интернет на 80% для общения в социальных сетевых сервисах[2].

За последние десять лет в обществе широко распространились социальные сетевые сервисы, и интерес к ним только растет. В связи с большим объемом вовлеченных пользователей социальные сетевые сервисы стали достаточно мощным инструментом воздействия на общество в целом и на отдельного индивидуума. Результатом роста социальных сетевых сервисов стали как позитивные следствия, связанные с решением актуальных проблем современного общества, так и негативные тенденции, характерные для общества сетевого типа, в частности манипулирование поведением больших групп социума, обсуждение антиобщественных мероприятий, разжигание межнациональной розни, пропаганда насилия и т. д. Примеры такого рода сайтов приведены на рис. 1 (а, б).



а)



б)

Рис. 1. Страницы социальной сети «ВКонтакте»
а) содержат группу о подрыве школы,
б) содержат информацию об использовании наркотиков

Поиском и удалением такой информации из социальных сервисов занимаются, как правило, администраторы системы, что требует довольно много времени. В связи с этим научные исследования и технологические разработки в области систем сетевого

семантического анализа высказываний крайне востребованы. Существует ряд разработок как зарубежных, так и отечественных, автоматизирующих эту деятельность, например: «Kaspersky Internet Security»[3], «ChildWebGuardian PRO»[4] и т. п. Разработанные системы не учитывают особенности архитектуры компьютера во время работы, в частности КЭШ-память[5], многоядерность системы[6] и возможности распределения вычислений[7].

Постановка задачи

Авторами статьи разработана мультиагентная система для сбора текстовой информации в сети МАС «Стоп-ТСН» (стоп – терроризм, суицид, наркотики), которая занимается сбором ссылок на страницы в Интернете, содержащие слова и выражения о наркотиках, суициде и терроризме. Разработанная система поможет родителям оградить детей от вредоносной информации, а также укажет спецслужбам на людей, угрожающих безопасности страны.

МАС «Стоп-ТСН» учитывает архитектуру компьютера, анализируя размер КЭШ-памяти и распределяя работу агентов на разные ядра процессора.

Для достижения поставленной цели был решен ряд взаимосвязанных задач в соответствии с жизненным циклом разработки ИС. Проведен анализ прикладной области, в том числе исследованы социальные сети, блоги, форумы, средства разработки мультиагентных систем и продукты-аналоги[8,9,10,11]; разработаны требования к МАС, проведено проектирование, реализация и отладка МАС «Стоп-ТСН»[12]. В данный момент прототип системы находится в стадии тестирования.

Проектирование архитектуры МАС и функциональности агентов

На рис. 2 приведена архитектура МАС «Стоп-ТСН», которая состоит из пяти агентов с разной функциональностью, двух баз данных, базы знаний и Центра обработки сообщений (ЦОС). В системе присутствуют механизмы для обмена информацией между агентами – очереди (queue)[13].

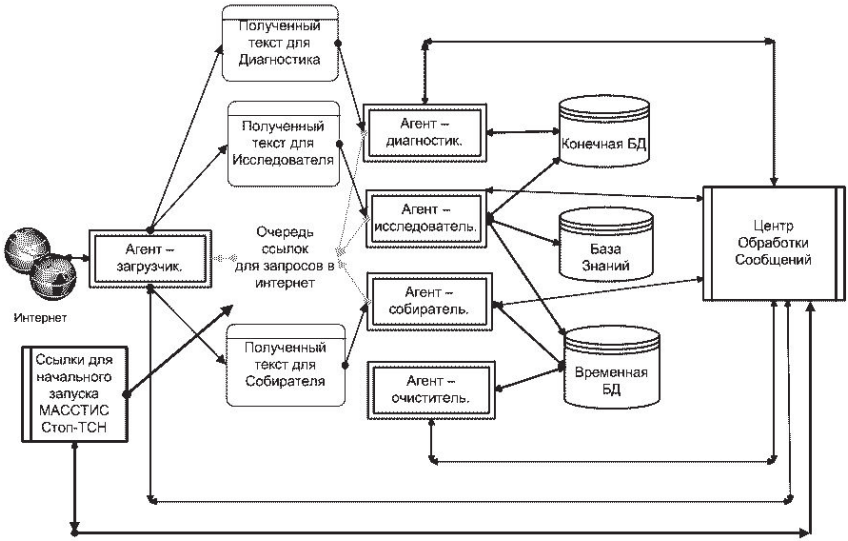


Рис. 2. Архитектура МАССТИС «Стоп-ТСН»

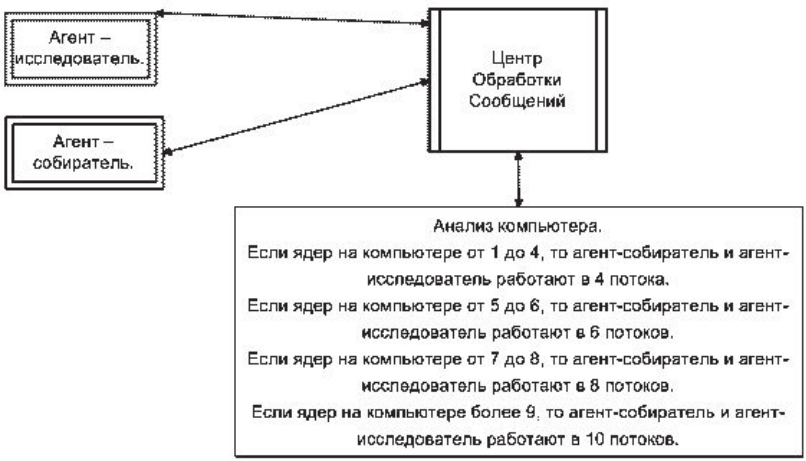


Рис. 3. Возможное количество потоков для агентов

ЦОС – единый центр, который занимается запуском и остановкой системы, вычисляет возможности компьютера, в частности размер КЭШ-памяти и количество ядер. Зная возможности компьютера, ЦОС указывает агенту-собирателю и агенту-исследователю количество потоков, которое они должны использовать для своей работы (рис. 3). Также ЦОС загружает начальный список опасных ссылок в «Очередь для запросов в Интернет» для первого запуска системы.

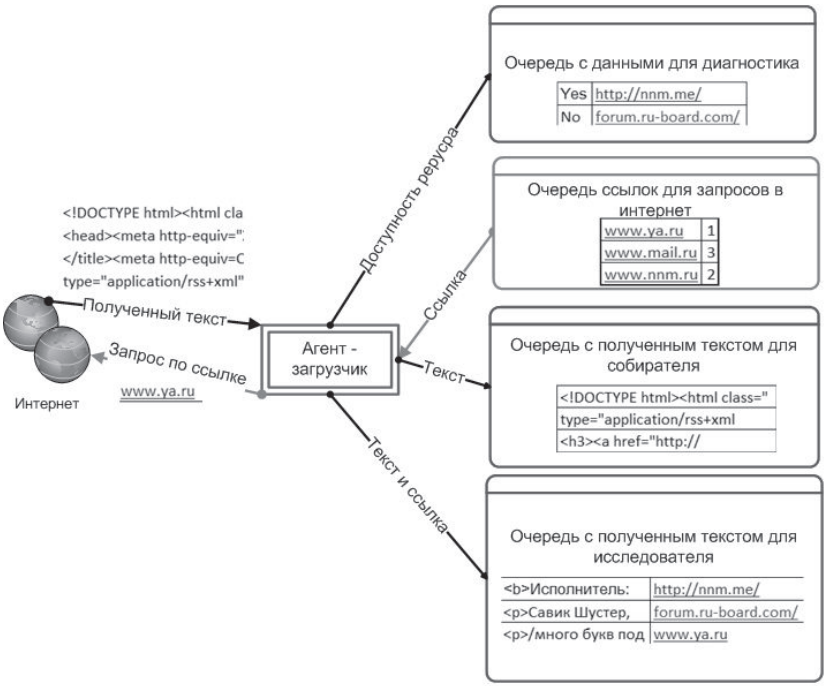


Рис. 4. Архитектура агента-загрузчика

Агент-загрузчик (рис. 4) переходит по ссылкам из «Очереди для запросов в Интернет» и загружает текст для каждого агента. Очередь для запросов в Интернет состоит из двух атрибутов. Первый – это ссылка, которую необходимо исследовать, а второй – это число, которое указывает, от какого агента пришла данная ссылка. Если 1, то собиратель, если 2, то исследователь, если 3, то диагностик. По второму атрибуту загрузчик определяет, в какую очередь

ему положить полученный текст из Интернета. Если 1, то в очередь для собирателя, если 2, то в очередь для исследователя, если 3, то в очередь для диагностика.

Агент-собиратель (рис. 5) из «Очереди с текстом для собирателя» получает новую порцию данных, которая содержит текст интернет-страницы. В полученном тексте агент ищет новые ссылки на страницы. Найденные ссылки агент сохраняет во временную базу данных и загружает в «Очередь для запросов в Интернет» для агента-загрузчика. Ссылки, сохраненные во «Временной БД», будут использованы агентом-исследователем и агентом-очистителем.

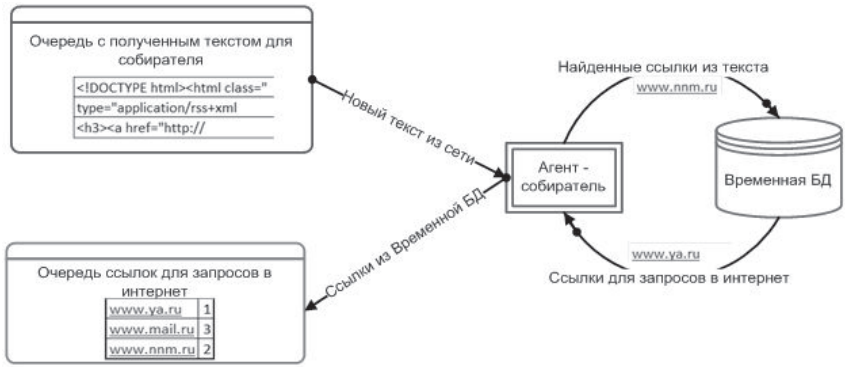


Рис. 5. Архитектура агента-собирателя

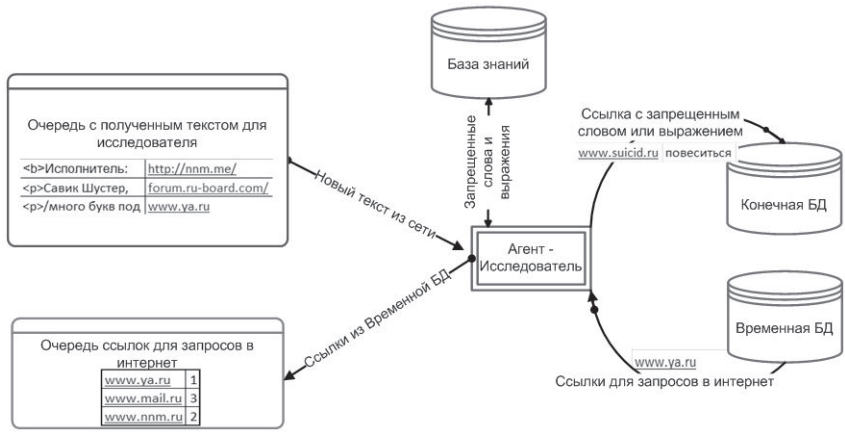


Рис. 6. Архитектура агента-исследователя

Агент-исследователь (рис. 6) из «Очереди с текстом для исследователя» получает новую порцию данных, которая содержит ссылку на страницу и текст со страницы. В полученном тексте агент ищет запрещенные слова и выражения из «Базы знаний». Если слова или выражения найдены, то он сохраняет ссылку на страницу в «Конечную базу данных». Также агент-исследователь загружает ссылки из «Временной БД» в «Очередь для запросов в Интернет» с целью получения текста со страницы.

Агент-диагностик проверяет работоспособность ссылок из «Конечной базы данных». Если ссылка не работает, то он ее удаляет.

Агент-очиститель удаляет ссылки, прочитанные агентом-исследователем из «Временной базы данных».

Временная база данных – это база, в которой хранятся ссылки, найденные агентом-собирателем в полученном тексте от агента-загрузчика и подлежащие дальнейшей обработке агентом-исследователем. Временная база данных состоит из 676 таблиц, причина выбора данного значения рассмотрена ниже. Каждая таблица имеет два атрибута (рис. 7):

- первый атрибут – это ссылка на исследуемый сайт;
- второй атрибут отвечает за прочтение ссылки агентом-исследователем. Если значение «1», то ссылка прочитана, «0» – нет.

narcoforum.com/t5963-muzhparenbrat-narkoman-vam-...	1
narcoforum.com/post247855.html#p247855	1
narcoforum.com/post247856.html#p247856	1
narcoforum.com/post247857.html#p247857	1
narcoforum.com/post247858.html#p247858	1
narcoforum.com/post247859.html#p247859	1
narcoforum.com/post247860.html#p247860	1
narcoforum.com/post247861.html#p247861	1
narcoforum.com/post247862.html#p247862	1
narcoforum.com/post247863.html#p247863	1

Рис. 7. Фрагмент таблицы временной базы данных

База знаний – это база, которая содержит словари запрещенных слов и выражений о суициде, наркотиках и терроризме (рис. 8).

База знаний содержит простейшую онтологию для проверки работоспособности МАС.

Word
героин
метадон
наркотик
соскочить
отходняк
наркоман

Word
взрыв произошел
ЦРУ
ФСБ
заложена бомба
тратил
взрывчатка

Word
грань между жизнью и смертью
сердце
ритуал совершить
мертвый
смысл жизни
способы суицида

Рис. 8. Словари базы знаний о суициде, терроризме и наркотиках

Конечная база данных – это база, которая содержит ссылки на страницы, на которых найдены слова или выражения из базы знаний (рис. 9). Конечная база данных состоит из трех таблиц:

- ссылки о суициде;
- ссылки о наркотиках;
- ссылки о терроризме.

Каждая таблица имеет два атрибута:

- ссылка на запрещенный сайт;
- запрещенное слово или выражение, найденное на странице.

http://news.revda.su/autonews/2831/#comments	ФСБ
http://news.revda.su/economics/2827/	ФСБ
http://news.revda.su/economics/2827/#comments	ФСБ
http://amt.allergist.ru/product/viktoza.html	ЦРУ
http://freemadbad.chat.ru/boom.htm	взорвать

Рис. 9. Фрагмент содержимого таблицы конечной базы данных

Исследование способов повышения производительности МАС

Для повышения быстродействия МАС «Стоп-ТСН» на этапе проектирования разработчиками было принято решение о распределении работы агентов на разные ядра процессора, а также учет размера КЭШ-памяти второго уровня. Существующие продукты-аналоги не используют многоядерность компьютера, поэтому время отображения страницы может быть увеличено от несколь-

ких миллисекунд до десятков секунд, что заставит пользователя отказаться от использования данного продукта.

Процессор сначала обращается к КЭШ-памяти в поисках информации для обработки, и если она не найдена, то через Системную Шину, как видно на рис. 10, обращается к оперативной памяти, что замедляет работу системы.

Рис. 10. Схема взаимодействия процессора с памятью

Учитывая размер КЭШ-памяти, можно ускорить работу программы в несколько раз. Существующие продукты-аналоги для первоначальной обработки информации используют одну большую базу данных, которая не сможет вся поместиться в КЭШ-памяти за один раз, как следствие, будут потери в производительности.

Разработчиками МАС «Стоп-ТСН» предложен другой подход, рассмотренный ниже. Известно, что КЭШ-память второго уровня напрямую влияет на производительность процессора. На современных компьютерах размер КЭШ-памяти второго уровня составляет 512 КБ (килобайт). У каждого ядра процессора своя КЭШ-память второго уровня. Создав вместо одной таблицы 676 таблиц по 1000 записей, можно добиться значительного прироста производительности. Учитывая количество ядер процессора, можно в несколько раз ускорить работу системы.

Временная база данных состоит из 676 таблиц – это 26*26. В английском алфавите 26 букв. Агент-собиратель анализирует первые две буквы ссылки и вносит ссылку в соответствующую таблицу (рис. 11).

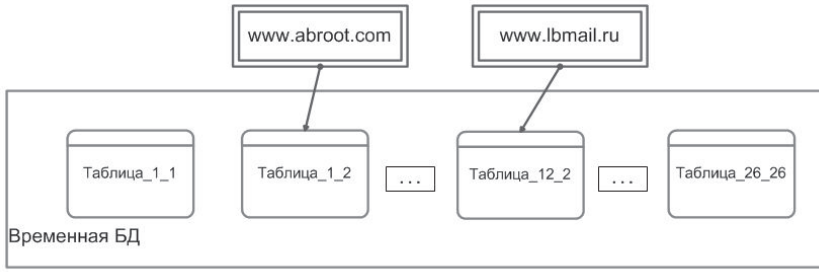


Рис. 11. Сохранение ссылки во временную базу данных

Тестирование производительности MAC с учетом КЭШ-памяти второго уровня

Для подтверждения высказанных предположений были проведены тесты производительности системы при разных размерах и количестве таблиц во временной БД.

Проведенное тестирование демонстрирует, что если в 100 таблиц по 1000 записей вносить изменения в несколько потоков с учетом КЭШ-памяти, то это окажется намного быстрее, чем работа с одной таблицей на 100 000 записей.

Тест 1.

Агент-собиратель работает в одном потоке и производит обработку и запись данных в БД с одной таблицей на 100 тыс. записей (рис. 12). Размер строки 55 символов, так как это средний размер ссылки в Интернете. Средний размер ссылки вычислен с помощью программы, написанной авторами статьи, которая исследовала 10 тыс. сайтов и вычислила средний размер ссылки.

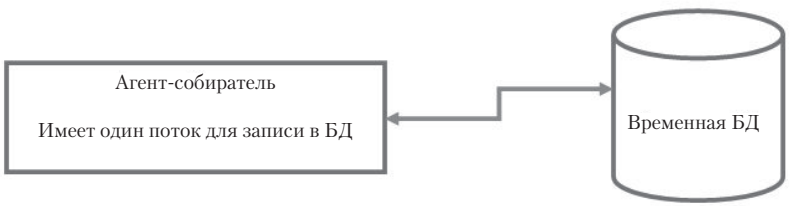


Рис. 12. Взаимодействие агента-собирателя с временной БД

Работа агента-собирателя завершается сообщением о времени, затраченном на запись (в сек.) (рис. 13). При этом на рис. 14 показана степень загруженности процессора (в %).

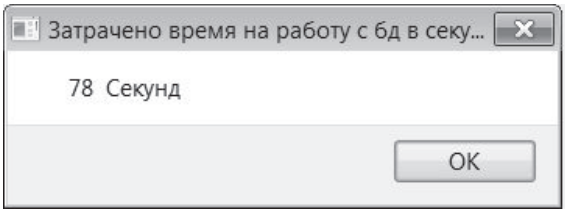


Рис. 13. Время, затраченное на запись

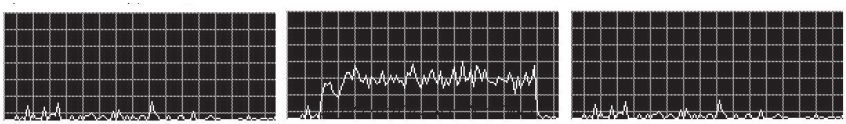


Рис. 14. Загрузка процессора

Из полученных данных следует, что только ***одно*** ядро процессора загружено на 45%, что явно недостаточно. Время, затраченное на работу с БД, 78 секунд. Возможности процессора позволяют выполнять больше операций.

Тест 2.

Во втором тесте исследована ситуация, при которой в БД создано 100 таблиц по 1000 записей. Как подтверждают результаты исследований, такая конфигурация работает намного эффективнее, так как есть возможность запустить несколько потоков и каждая таблица может быть загружена в КЭШ-память за один раз. На рис. 15 показана схема взаимодействия агента-собирателя с временной БД, в которой агент-собиратель имеет 6 потоков для взаимодействия с БД.

Полученные результаты тестирования представлены на рис. 16 и 17. Загрузка процессора во время работы на всех ядрах составляет 90%, что указывает на правильное использование ресурсов компьютера.

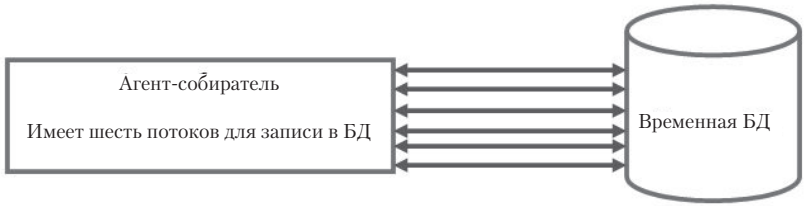


Рис. 15. Взаимодействие агента-собирателя с временной БД

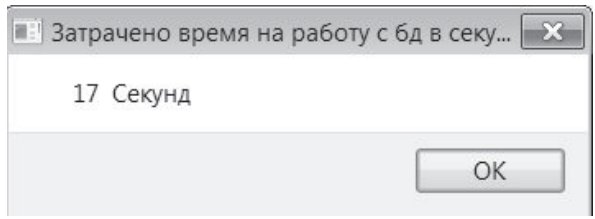


Рис. 16. Время, затраченное на запись в БД

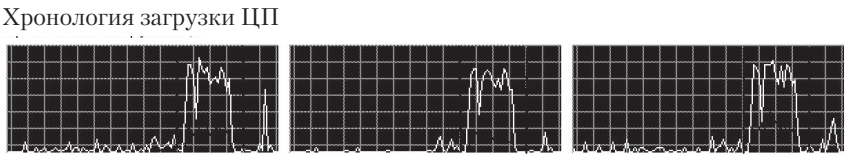


Рис. 17. Загрузка процессора

Из рис. 13 и 16 видна разница в скорости выполнения записи, в 4,5 раза быстрее происходит запись в «малые» таблицы, чем в одну большую, что обусловлено 90-процентной загрузкой всех трех ядер (рис. 17), по сравнению с 45-процентной загрузкой единственного ядра процессора (тест 1), что говорит об оптимальном выборе количества потоков и размере таблиц для данного многоядерного компьютера.

Выводы

Разработана мультиагентная система для сбора текстовой информации в сети «Стоп-ТСН», которая занимается сбором ссылок

на «опасные / вредоносные» страницы в Интернете, содержащие информацию, связанную с терроризмом, суицидом и наркотиками.

Проведено проектирование архитектуры МАС, агентов системы, баз данных, механизмов доступа в глобальную сеть, выбраны средства реализации проекта, осуществлена реализация МАССТИС «Стоп-ТСН».

Проектируемая МАС учитывает многоядерность архитектуры компьютера, анализируя размер КЭШ-памяти и распределяя работу агентов на разные ядра процессора, что позволяет в разы ускорить работу программы. Преимущества разработанной системы по сравнению с существующими рассмотрены на конкретных примерах.

Разработанная система поможет родителям оградить детей от такой информации, а также укажет спецслужбам на людей, угрожающих безопасности страны.

Примечания

1 Для чего люди используют интернет? [Электронный ресурс] // Фонд «Общественное мнение». URL: http://fom.ru/SMI-i-internet/11088 (дата обращения: 23.11.2014).

2 Социальные сетевые сервисы [Электронный ресурс] // Академик. URL: http://dic.academic.ru/dic.nsf/ruwiki/1334827 (дата обращения: 23.11.2014).

3 Kaspersky Internet Security [Электронный ресурс] // Wikipedia. URL: https://ru.wikipedia.org/wiki/Kaspersky_Internet_Security (дата обращения: 23.11.2014).

4 Интернет фильтр «ChildWebGuardian Pro» [Электронный ресурс]. URL: http://www.childwebguardian.ru (дата обращения: 23.11.2014).

5 *Антес Г.* Кэш-память (Computerworld Россия. 2000. № 15) [Электронный ресурс] // Открытые системы. URL: http://www.osp.ru/cw/2000/15/4418/ (дата обращения: 23.11.2014).

6 Сравнение многоядерных процессоров [Электронный ресурс] // HardwareGuide.ru. URL: http://hardwareguide.ru/%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80/mnogojadernie-processori/ (дата обращения: 23.11.2014).

7 *Таненбаум Э., Ван Стеен М.* Распределенные системы. Принципы и парадигмы. СПб.: Питер, 2003. 877 с.: ил.

8 *Пестряев А.А., Воронова Л.И.* Анализ поисковых роботов и выбор функций для своего робота // Мат-лы V Междунар. студенч. электрон. науч. конф. «Студенческий научный форум» [Электронный ресурс]. URL: http://www.scienceforum.ru/2013/183/2549 (дата обращения: 23.11.2014).

[9] *Лукоянов И.А., Охапкина Е.П., Воронов В.И., Воронова Л.И.* Разработка и внедрение поискового робота для анализа интересов клиентов // Современные наукоемкие технологии. 2014. № 5-2. С. 210–212.

[10] *Авхадеев Б.Р., Воронова Л.И., Охапкина Е.П.* Разработка рекомендательной системы на основе данных из профиля социальной сети «ВКОНТАКТЕ» // Вестник Нижневартовского государственного университета. 2014. № 3. С. 68–76.

[11] *Охапкина Е.П., Воронова Л.И.* Разработка фрагмента онтологии для многоагентной системы модерации сообщений пользователей // Там же. С. 60–67.

[12] *Пестряев А.А., Воронова Л.И.* Мультиагентная система. Взаимодействие агента-собирателя с базой данных // Современные наукоемкие технологии. 2014. № 5–2. С. 214–217.

[13] *Хомутова Е.В., Воронова Л.И.* Автоматизация ранжирования типов визуализации в DATA MINING для нереляционных баз данных // Там же. С. 219–221.

С.В. Запечников

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ АНАЛИТИЧЕСКОГО, ЧИСЛЕННОГО И ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ

В статье сообщается о разработке программного комплекса для моделирования систем массового обслуживания. Особенность программного комплекса состоит в том, что он позволяет моделировать многие виды систем массового обслуживания, в том числе составлять из элементарных систем более сложные, и для каждого типа систем проводить как аналитическое (или численное), так и имитационное моделирование. Сравнение результатов, полученных с помощью совершенно разных по своей природе моделей, позволяет убедиться в их адекватности. Основная сфера применения программного комплекса – расчет и прогнозирование показателей доступности, надежности, отказоустойчивости и производительности сложных вычислительных систем, в том числе основанных на «облачных» технологиях.

Ключевые слова: системы массового обслуживания, аналитическое моделирование, имитационное моделирование, доступность, показатели производительности.

Введение

Активное развитие в последнее время распределенных вычислительных систем в различных формах (кластеры, грид-системы, «облачные технологии», локальные и глобальные компьютерные системы) актуализирует проблему обеспечения одного из главных аспектов информационной безопасности (наряду с конфиденциальностью и целостностью) – доступность сервисов, предоставляемых вычислительными системами, и обрабатываемой на них информации. Доступность – многоаспектное понятие: чтобы оце-

нить доступность информационной системы, необходимо получить оценки показателей надежности, катастрофоустойчивости системы обработки данных, своевременности обработки информации и др. Эти показатели связаны неоднозначным образом: более сложная система может быть более производительной, но менее надежной. Своевременность обработки информации зависит не только напрямую от производительности системы, но и от организации вычислительного процесса (алгоритмов распределения задач, возможности «эластично» масштабировать систему и проч.). Возможности гибкой организации вычислительного процесса значительно расширились с развитием облачных технологий. Необходимость проведения исследований в этой области обусловлена недостаточно эффективным использованием существующих возможностей гибкой организации вычислительного процесса в распределенных вычислительных системах, в особенности построенных на основе облачных технологий, которые могут быть применены в качестве платформы для решения задач аналитической обработки «больших данных» и других задач.

Структура и функции программного комплекса

Теоретической и методологической базой исследований являются теория случайных процессов, теория массового обслуживания, практика имитационного моделирования, в том числе на основе агентного подхода. Современная вычислительная техника, языки программирования высокого уровня и специализированные библиотеки предоставляют очень широкие возможности в области создания аналитических, численных и имитационных моделей систем массового обслуживания. Вместе с тем за последние годы российская наука допустила значительное отставание от мировых достижений в области моделирования систем массового обслуживания. Преодоление этого отставания позволит не только решать задачи эффективного использования компьютерной техники и информационных систем на ее основе, но также в силу универсальности результатов, получаемых при анализе систем массового обслуживания, использовать их в других областях деятельности после настройки соответствующих параметров систем массового обслуживания.

Создание инструментальной базы исследований заключается в разработке универсального программного комплекса для аналитического, численного и имитационного моделирования систем массового обслуживания.

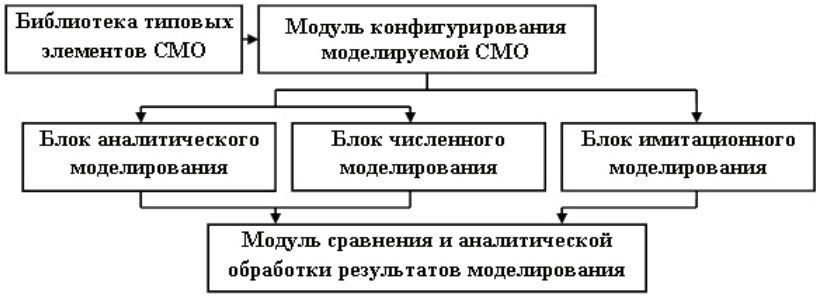


Рис. 1. Структурно-функциональная схема программного комплекса моделирования СМО

Общую идею программного комплекса отражает рис. 1. Программный комплекс имеет библиотеку типовых элементов систем массового обслуживания (СМО). Общепринятой является символическая нотация: так, например, *M/M/1* – система с потоком требований, имеющим экспоненциальное распределение интервалов между временем поступления требований, экспоненциальным временем обслуживания и одним обслуживающим устройством с отказами, *M/G/n/k* – система с потоком требований, имеющим экспоненциальное распределение интервалов между временем поступления требований, экспоненциальным временем обслуживания, *n* обслуживающими устройствами и накопителем емкостью *k* требований и т. п. Для каждого типового или заданного пользователем элемента СМО программный комплекс позволяет выполнить аналитическое и имитационное моделирование, при невозможности выполнить аналитическое моделирование взамен него выполняется численное. Результаты моделирования визуализируются путем построения двух семейств графиков на одном поле: первое семейство отражает результаты аналитического (численного) моделирования при заданных пользователем значениях параметров системы, собранной из типовых элементов, второе – результаты имитационного моделирования той же системы. Визуальный или статистический анализ точек, принадлежащих двум семействам графиков, позволит пользователю сделать выводы об адекватности аналитической (численной) модели, предложенной для описания интересующей его СМО.

Таким образом, программный комплекс должен стать прежде всего инструментом исследователя, работающего в области анализа показателей доступности, отказоустойчивости и надежности сложных вычислительных комплексов и информационных систем.

Модуль аналитического и численного моделирования

Теоретической основой построения аналитических моделей СМО служит теория массового обслуживания (в англоязычной литературе называемая обычно теорией очередей – queueing theory). Для каждого типа моделируемых СМО строится своя собственная аналитическая модель. Различают два вида моделей:

1) модели, основанные на вычислении функций плотности распределения времени между поступлением заявок на обслуживание, времени обслуживания заявок и проч.;
2) модели, основанные на построении модели марковского (полумарковского) процесса, реализуемого в данной СМО, и оценке вероятностей перехода марковской цепи из одного состояния в другое.

В зависимости от моделируемой СМО бывает удобным придерживаться то одной, то другой модели. Для некоторых, обычно сравнительно простых СМО возможно даже построить одновременно модели, реализующие оба подхода, а затем сравнить результаты, получаемые с помощью каждой из них, что служит дополнительной гарантией корректности результатов. Однако чаще все же встречается ситуация, когда применяются модели второго типа, если построение модели первого типа наталкивается на невозможность вычисления в аналитической форме какого-либо интеграла в формуле, описывающей плотности распределения вероятностей. В том случае, когда и для модели второго типа не может быть получено точное решение, применяется численное моделирование: вместо точных методов решения систем уравнений для получения результатов используются приближенные численные методы. Адекватность и точность численной модели проверяются по степени соответствия полученного решения результатам имитационного моделирования (см. ниже).

Принципиальное различие между двумя типами моделей заключается в следующем. В первом случае модель описывает «внешнюю», физически наблюдаемую сторону процессов, например время между поступлением требований в очередь и выборкой их из очереди, происходящей одновременно с началом обслуживания требований. Во втором случае модель описывает «внутреннюю», ненаблюдаемую природу системы, которая описывается в абстрактных терминах состояний и переходов между ними.

На рис. 2 приведен пример пользовательского интерфейса для задания параметров моделируемой СМО типа *M/G/1/k* и выбора графиков, которые будут отображаться по результатам моделирования.

В качестве параметров аналитической (численной) модели пользователем могут быть указаны значения:

- интенсивности входящего потока требований;
- интенсивности обработки требований одним обслуживающим устройством (если обработка многофазная, то на каждой из фаз обслуживания);
- количества обслуживающих устройств;
- количества мест в очереди к обслуживающему устройству.

Получаемые с помощью программного комплекса результаты моделирования могут выражаться четырьмя семействами графиков:

- графики пропускной способности СМО;
- графики коэффициента потери требований из-за недоступности СМО;
- графики коэффициента полезного использования обрабатывающих устройств;
- графики средней задержки требований в СМО.

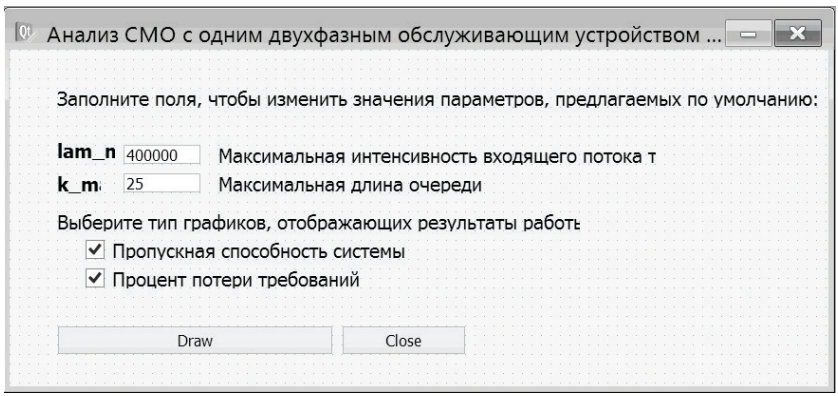


Рис. 2. Окно пользовательского интерфейса для задания параметров моделируемой СМО типа *M/G/1/k* и выбора отображаемых результатов моделирования

На рис. 3 приведены примеры графиков, полученных для СМО типа *M/G/1/25,* т. е. СМО с пуассоновским входящим потоком требований, очередью на 25 требований и одним обслуживающим устройством с произвольным временем обслуживания. В данном случае взято так называемое двухфазное обслуживающее устройство, когда обслуживание требования состоит из двух последовательных этапов, каждый из которых описывается экспоненциальным законом распределения, но обработка следующего требования

может быть начата не раньше, чем закончится последняя фаза обслуживания предыдущего требования. Это семейство графиков было построено с целью верификации результатов, получаемых с помощью разрабатываемого программного комплекса, на основе сравнения их с результатами К. Салаха[1].

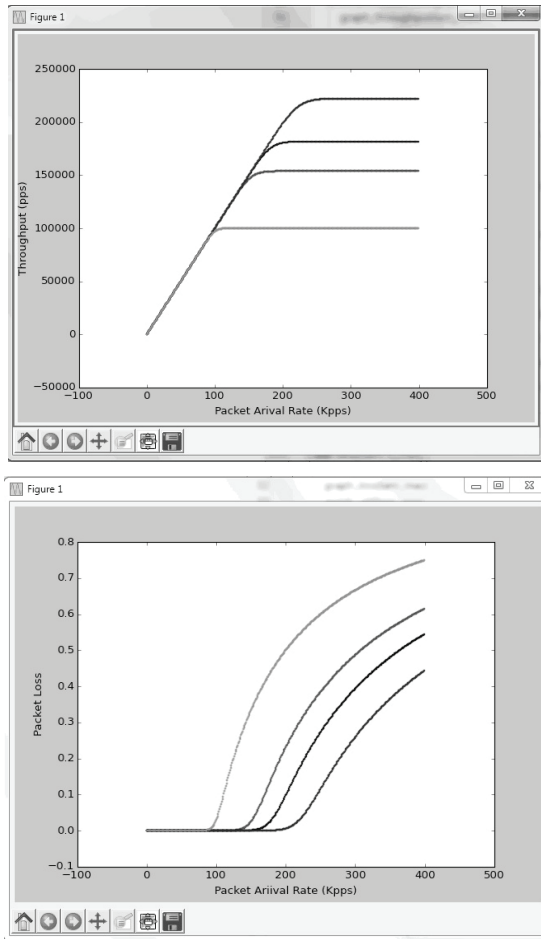


Рис. 3. Примеры графиков с результатами аналитического моделирования СМО типа *M/G/1/25*: зависимости потока исходящих требований и доли отклоненных требований от интенсивности потока входящих требований

В показанном на рис. 3 примере для построения каждого графика вычисляется 400 точек, для получения каждой точки решается система разностных уравнений 25-го порядка. Плотность точек графика может настраиваться пользователем (чем выше плотность, тем, разумеется, большим будет время вычисления точек графика). Порядок системы уравнений зависит от числа мест в очереди и, таким образом, является функцией параметров модели.

Функционально программный модуль аналитического моделирования состоит из блока, реализующего графический пользовательский интерфейс, и блока, выполняющего вычисления, необходимые для построения графиков. На рис. 4 приведена блок-схема работы графического интерфейса.

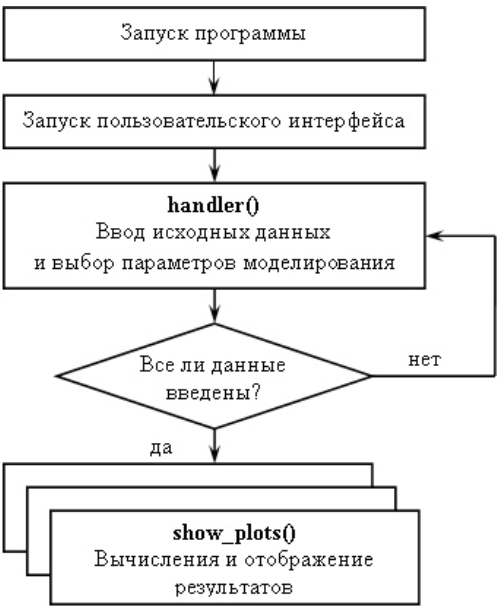


Рис. 4. Блок-схема работы
графического интерфейса пользователя

На рис. 5 показан принцип работы вычислительного блока. Каждая вычислительная процедура «обернута» в процедуру построения семейства графиков, отображающего результаты вычислений. Построение каждого семейства графиков выполняется

лишь в том случае, если пользователем выбрано отображение соответствующего результата моделирования.

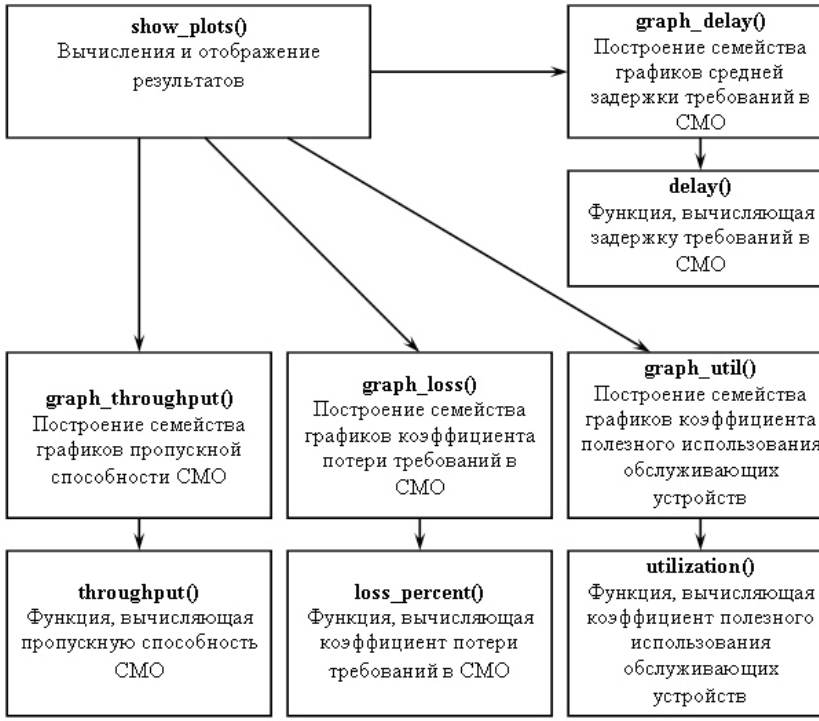


Рис. 5. Блок-схема вычислительной части программного модуля аналитического и численного моделирования

Модуль имитационного моделирования

Модуль имитационного моделирования в составе программного комплекса имеет еще более сложную структуру, чем модуль аналитического моделирования, и решает многообразные функциональные задачи. Основные компоненты модуля имитационного моделирования (структуры данных и подпрограммы) таковы[2]:

- состояние системы – набор переменных состояния, которые необходимы для описания моделируемой СМО в конкретный момент времени;

- часы модельного времени – указывает текущее значение времени;
- список событий – список, который содержит время возникновения каждого последующего типа событий (например, поступление требования в систему, поступление требования на обслуживание, уход требования из системы и проч.);
- статистические счетчики – ряд переменных, задействованных для хранения информации о характеристиках системы;
- программа инициализации – подпрограмма, которая устанавливает имитационную модель в исходное состояние в момент времени «ноль»;
- синхронизирующая программа – подпрограмма, находящая следующее событие в списке событий и переводящая часы на время возникновения этого события;
- программа обработки событий – подпрограмма, которая обновляет состояние системы, когда происходит событие определенного типа;
- программы библиотеки – ряд подпрограмм, которые применяются для генерации случайных наблюдений из распределений вероятностей, которые были определены как часть имитационной модели;
- генератор отчетов – подпрограмма, считывающая со статических счетчиков оценки критериев оценки и выдающая отчет в конце моделирования;
- основная (управляющая) программа – подпрограмма, вызывающая синхронизирующую программу для определения следующего события и передающая управление соответствующей событийной программе для обеспечения заданного обновления состояния системы. Она может осуществлять контроль необходимости прекращения моделирования и вызывать генератор отчетов.

В разрабатываемом программном комплексе (как и в большинстве программ имитационного моделирования) используется прием продвижения времени от события к событию. В исходном состоянии модельное время устанавливается в значение, равное нулю, и определяется время возникновения следующих событий. Затем часы перейдут на время, когда возникнет следующее ближайшее событие, и состояние системы в этот момент обновится, здесь будут учтены произошедшее событие и сведения о времени возникновения будущих событий. Затем производятся те же действия и т. д. Этот процесс будет продолжаться до тех пор, пока не возникнет заранее указанное условие останова. В дискретно-собы-

тийной модели изменения состояний происходят только во время возникновения событий, поэтому периоды бездействия пропускаются. Длительность интервала продвижения модельного времени от одного события к другому различна.

Структура модуля имитационного моделирования выстроена исходя из принятого принципа продвижения модельного времени «от события к событию». Структурная схема модуля показана на рис. 6. Она практически полностью соответствует классическому подходу В. Кельтона и А. Лоу[3].

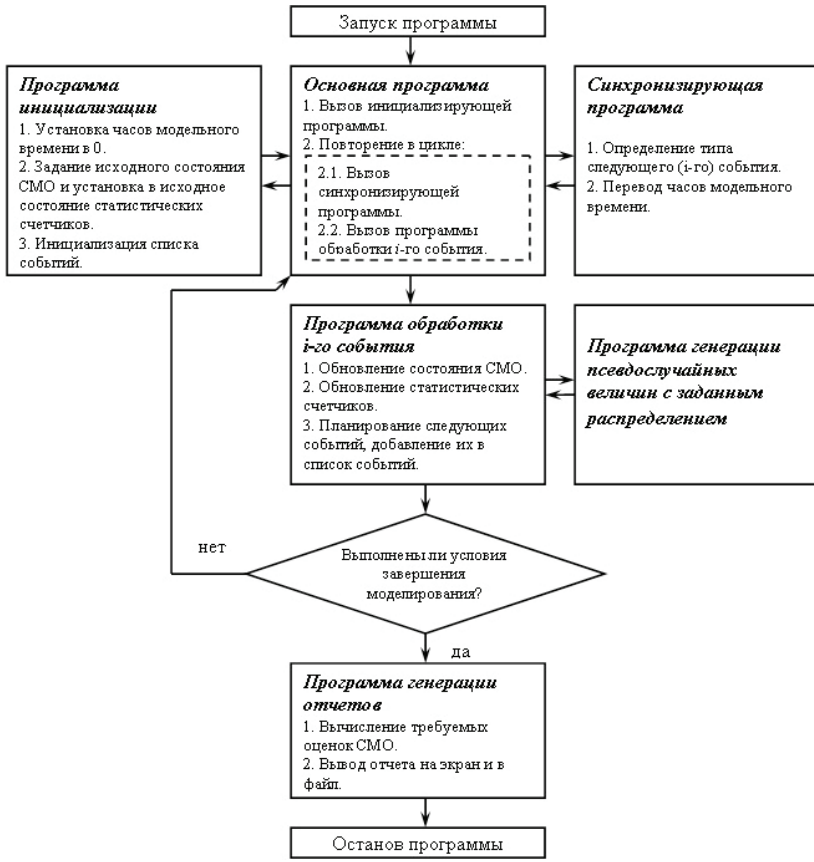


Рис. 6. Структура модуля имитационного моделирования

Одним из основных условий получения достоверных результатов имитационного моделирования является генерация большого количества случайных величин с заданными распределениями вероятностей.

Предварительно проведенные эксперименты показали, что распределения вероятностей, полученные с использованием встроенного в язык программирования Python генератора псевдослучайных чисел, весьма далеки от требуемых для целей имитационного моделирования. В язык программирования, как правило, встроена лишь возможность генерации равномерно распределенных на заданном интервале чисел. Псевдослучайные величины с другими распределениями получаются из равномерно распределенных с использованием специальных методов. Несмотря на хорошие статистические показатели встроенного в язык Python генератора равномерно распределенных псевдослучайных величин, любые другие распределения, полученные путем преобразования выхода псевдослучайного генератора, лишь с большой долей условности можно соотносить с ожидаемыми, например с экспоненциальным (рис. 7) или с нормальным (рис. 8). Поэтому их правильнее было бы назвать квазиэкспоненциальным и квазинормальным. Качественный генератор не должен давать столь больших выбросов на гистограмме. В связи с этим возникает необходимость разработки собственного генератора, обладающего более качественными статистическими характеристиками.

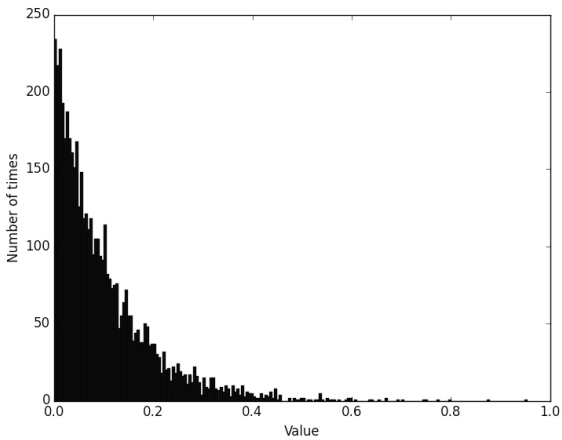


Рис. 7. Квазиэкспоненциальное распределение случайной величины, полученное с использованием встроенного генератора случайных чисел языка Python

С целью соответствия жестким требованиям к качеству генерации случайных величин для программного комплекса реализован многоканальный псевдослучайный генератор в соответствии с методом, описанным В. Кельтоном и А. Лоу[4].

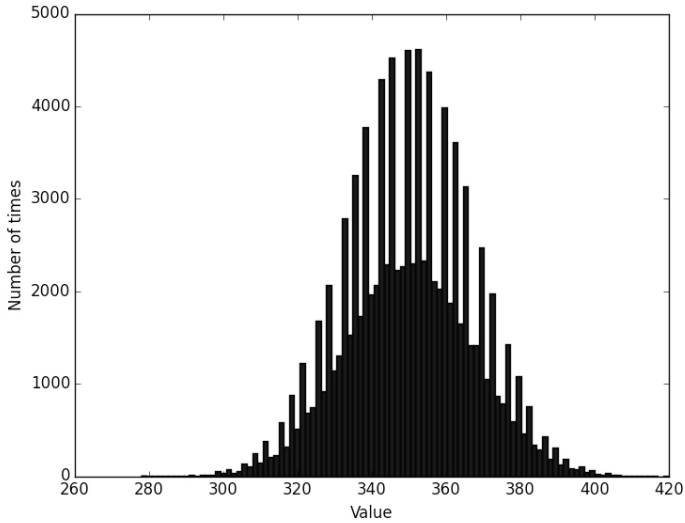


Рис. 8. Квазинормальное распределение случайной величины, полученное с использованием встроенного генератора случайных чисел языка Python

Состояние и перспективы разработки

В настоящее время ведется разработка первой очереди программного комплекса, которая должна завершиться созданием отдельных программных модулей для аналитического (численного) и имитационного моделирования СМО, визуализации результатов, а также пользовательского интерфейса. Вторая очередь разработки будет состоять в разработке оставшихся модулей, их интеграции в программный комплекс и создании библиотеки типовых элементов СМО, из которых пользователь сможет создавать сложные СМО интересующей его конфигурации.

Языком разработки является Python 3.2. Для реализации модулей аналитического и численного моделирования применяется библиотека NumPy, для визуализации результатов моделирования – библиотека matplotlib, для реализации пользовательского интерфейса – библиотека PyQt4. Разработку модуля имитационного моделирования в дальнейшем предполагается вести с использованием библиотеки SimPy – библиотеки дискретно-событийного моделирования для языка Python, чтобы упростить реализацию функций координации синхронно протекающих процессов в сложной системе.

Завершение создания программного комплекса сделает возможным постановку экспериментов по анализу и сценарному прогнозированию поведения массово-параллельных вычислительных систем, построенных на базе технологий виртуализации, в частности экспериментов с целью исследования:

- характеристик потоковой обработки «больших данных» в режиме реального времени;
- свойств «эластичности» вычислительных систем, т. е. способности их гибко менять состав и количество оборудования, задействованного в обработке данных, при изменении интенсивности потока входящих требований;
- возможностей противодействие DDoS-атакам.

Этим списком далеко не исчерпывается перечень возможных областей применения программного комплекса. Полученные с помощью программного комплекса результаты способны значительно повысить эффективность процессов проектирования и создания центров обработки данных, а также частных «облаков» крупных корпораций.

Примечания

1 *Salah K.* Analysis of a two-stage network server // Applied Mathematics and Computation. 2011. № 217. P. 9635–9645.

2 *Кельтон В., Лоу А.* Имитационное моделирование. Классика CS. 3-е изд. СПб.: Питер; Издат. группа BHV, 2004. 874 с.

3 Там же. С. 28–29.

4 Там же. С. 30–31.

А.С. Зайцев, А.А. Малюк

СИСТЕМНО-ДИНАМИЧЕСКОЕ МОДЕЛИРОВАНИЕ УГРОЗЫ КРАЖИ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

В статье предложена классификация внутренних угроз информационной безопасности, рассмотрен метод прогнозирования развития инсайдерских угроз при помощи системно-динамического моделирования, разработаны прогнозные поведенческие модели для угроз кражи интеллектуальной собственности в целях получения деловых преимуществ в одиночку и с соучастниками.

Ключевые слова: системная динамика, поведенческие модели, имитационное моделирование, внутренний нарушитель, интеллектуальная собственность.

Введение

Исследования в области обеспечения информационной безопасности (ИБ) до недавних пор концентрировались в основном на противодействии внешним угрозам ИБ, в этих целях на сегодняшний день разработан значительный арсенал методов и средств технологического характера, стандарты и лучшие практики, претерпевшие несколько циклов совершенствования и в достаточной мере обеспечивающие защиту при правильном внедрении.

Вопрос защиты информационных активов и информационно-телекоммуникационной инфраструктуры (ИТ-инфраструктура), организации от внутренних угроз ИБ не имеет технологического решения и лежит в плоскости организационных мер гуманитарного характера. Ввиду этого на данный момент не существует общепринятых подходов к защите информационных активов и ИТ-инфраструктуры от внутреннего нарушителя ИБ.

Проблема защиты информации от внутреннего нарушителя является одной из наиболее сложных проблем в области ИБ, так как зависит от психологических и поведенческих аспектов, которые с трудом поддаются оценке и прогнозированию со стороны руководства. К примеру, введение санкций по отношению к нарушителю ИБ, по мнению руководства, должно привести к нейтрализации внутренней угрозы, но фактически зачастую приводит к эскалации конфликта и повышению вероятности реализации атаки саботажа с использованием информационных систем организации (ИТ-саботаж). Поэтому крайне важной научной задачей является поддержка принятия решений по реагированию на потенциальные внутренние угрозы ИБ на основе использования поведенческих моделей нарушителя.

В качестве метода для моделирования внутреннего нарушителя ИБ целесообразно использовать системную динамику Дж. Форрестера[1]. Данный метод был впервые применен для исследования внутренних угроз ИБ в 2003 г. научным коллективом Carnegie Mellon University Software Engineering Institute CERT Insider Threat Team (CERT)[2], который исследовал информацию об инцидентах с участием внутренних нарушителей ИБ, полученную в открытых источниках, разработал классификацию внутренних угроз ИБ и диаграммы причинно-следственных связей (ДПСС) для всех выделенных классов угроз. Несмотря на то что полученные CERT диаграммы позволяют лучше понять поведение внутреннего нарушителя ИБ, с их помощью невозможно произвести компьютерное моделирование и прогнозирование.

Независимо от CERT системно-динамическое моделирование как метод исследования внутренних угроз ИБ был применен в работе[3], в которой была разработана системно-динамическая диаграмма или диаграмма потоков (ДП), единая для всех внутренних угроз ИБ, но компьютерного моделирования также не было проведено.

В настоящей статье рассматривается метод прогнозирования потенциального поведения внутреннего нарушителя ИБ при помощи системно-динамического моделирования, разработаны прогнозные модели для угроз кражи интеллектуальной собственности (ИСб) в целях получения деловых преимуществ с соучастниками и в одиночку, а также приведены результаты тестового моделирования.

Разработка системно-динамических моделей внутреннего нарушителя информационной безопасности

Системно-динамическое моделирование любой системы, в том числе поведения внутреннего нарушителя ИБ в организации, состоит из следующих последовательных стадий.

1. Построение схемы взаимодействия основных элементов системы. На данной стадии необходимо исследовать поведение внутреннего нарушителя ИБ в организации и выделить основные кластеры факторов, влияющих на развитие внутренней угрозы ИБ.

2. Разработка ДПСС. На данной стадии необходимо детализировать основные элементы системы и их взаимодействие в виде причинно-следственных связей (ПСС), получив тем самым совокупность взаимодействующих факторов (параметров системы), определяющих поведение внутреннего нарушителя ИБ, в форме ориентированного графа. ПСС будем считать положительной, если увеличение (уменьшение) влияющего параметра системы вызывает увеличение (уменьшение) параметра, на который оказывается влияние. Если увеличение влияющего параметра системы вызывает уменьшение параметра, на который оказывается влияние, то ПСС будем считать отрицательной. Параметры системы и ПСС образуют петли обратной связи (ПОС), определяющие поведение внутреннего нарушителя ИБ. ПОС по своему характеру влияния на развитие системы также могут быть разделены на отрицательные и положительные, отрицательная ПОС стабилизирует состояние системы, положительная – ускоряет динамику изменения параметров системы. Характер ПОС определяется числом входящих в нее отрицательных ПСС: нечетное число отрицательных ПСС формирует отрицательную ПОС, четное – положительную ПОС. Элементы, не входящие в ПОС, являются экзогенными и должны задаваться аналитиком в процессе моделирования.

3. Разработка ДП. На данной стадии необходимо преобразовать ДПСС в форму системно-динамической диаграммы (ДП). Параметр, на который оказывается влияние большого числа других параметров посредством как положительных, так и отрицательных ПСС, целесообразно выделить в виде уровня. Специальные параметры ДП – темпы вызывают увеличение или уменьшение уровня. При необходимости можно использовать дополнительные элементы ДП – константы, переменные, таблицы и проч.

4. Задание параметров системы и тестовое моделирование. На данной стадии аналитиком задаются параметры системы, причем

целесообразно определить относительную значимость основных ПОС ДП и на основании этого задать характеристики ПСС, проверяя поведение системы на краевых значениях начальных параметров, в которых поведение внутреннего нарушителя ИБ зачастую очевидно. В некоторых случаях проводить отладку ДП целесообразно на уровне одного или нескольких элементов системы. Далее необходимо провести тестовое моделирование, подтверждающее или опровергающее адекватность полученной модели.

Поведение внутреннего нарушителя ИБ в корне отличается в зависимости от того, какую угрозу ИБ он реализует. Ввиду этого целесообразно производить моделирование каждой внутренней угрозы ИБ в отдельности.

Классификация внутренних нарушителей ИБ приведена в табл. 1.

Таблица 1

Классификация внутренних угроз ИБ

Внутренняя угроза ИБ	Мотив нарушителя	Предполагается увольнение	Сговор внутренний	Сговор внешний
Саботаж	Обида	Не всегда	Нет	Нет
Шпионаж	Деньги Обида	Нет	Нет	Да
Мошенничество на руководящей должности	Деньги	Нет	Нет Социальная инженерия	Нет
Мошенничество на неруководящей должности	Деньги	Нет	Нет	Не всегда
Кража интеллектуальной собственности (ИСб) в целях получения деловых преимуществ в одиночку	Бизнес-преимущества Обида	Да	Нет	Да
Кража ИСб в целях получения деловых преимуществ с соучастниками	Бизнес-преимущества	Да	Да	Да
Халатное немотивированное нарушение ИБ	Нет	Нет	Нет	Нет
Манипулируемое немотивированное нарушение ИБ	Нет	Нет	Нет	Социальная инженерия

Дадим некоторые определения.

Внутренний нарушитель ИБ – текущий или бывший сотрудник организации, подрядчик или бизнес-партнер, который имеет или имел авторизованный доступ к сетям, системам или данным организации и превысил или использовал этот доступ таким образом, что нарушил конфиденциальность, целостность или доступность информации или ИС организации. Злоумышленный внутренний нарушитель ИБ намеренно нарушает ИБ организации и имеет мотив. Немотивированный (незлоумышленный) внутренний нарушитель ИБ нарушает ИБ организации ненамеренно.

Саботаж (ИТ-саботаж) – угроза ИБ, использование внутренним нарушителем ИБ информационных систем (ИС) организации для нанесения вреда организации или конкретному сотруднику[4].

Кража ИСб в целях получения деловых преимуществ – угроза ИБ, кража конфиденциальной информации или ИСб организации внутренним нарушителем ИБ для использования ее на новой работе, для нахождения новой работы или организации собственного предприятия[5].

Мошенничество – угроза ИБ, использование внутренним нарушителем ИБ ИС организации для неавторизованного использования, модификации или удаления данных организации (в том числе, кража персональных данных) с целью получения дохода. К мошенничеству не относятся случаи промышленного и международного шпионажа[6].

Шпионаж (ИТ-шпионаж) – угроза ИБ, использование внутренним нарушителем ИБ ИС организации для сбора и передачи информации внешней стороне (конкурирующей организации или иностранному государству) в целях выгоды для внешней стороны без намерения покинуть организацию после передачи информации. Если внешняя сторона является конкурирующей организацией, то применяется термин «промышленный шпионаж». Если внешняя сторона является иностранным государством, то применим термин «международный шпионаж».

Термины «инсайдер» и «внутренний нарушитель» равнозначны.

На основе проанализированных исследований, а также информации об инцидентах ИБ с участием внутренних нарушителей, полученной из открытых источников, разработаны типовой сценарий развития инсайдерского правонарушения и схема взаимодействия основных элементов системы поведения внутреннего нарушителя ИБ, единая для всех внутренних угроз ИБ.

Ключом для совершения правонарушения является мотивация внутреннего нарушителя ИБ. Для угрозы шпионажа, кражи ИСб в целях получения деловых преимуществ в одиночку и с

соучастниками, а также для части сценариев мошенничества на неруководящей должности с мотивацией связан сговор с внешней стороной. Внутренний нарушитель ИБ проверяет, достаточно ли у него полномочий (технических возможностей) для реализации угрозы, и при недостатке прибегает к внутреннему сговору (для угрозы кражи ИСб в целях получения деловых преимуществ с соучастниками) или к манипуляции подчиненными (для угрозы мошенничества на руководящей должности). Поведение инсайдера, которое может нанести ущерб организации, также дает ей возможность получить информацию о реализации угрозы ИБ. Организация может различным образом реагировать на потенциальную или реализованную угрозу ИБ. Одним из вариантов санкций по отношению к внутреннему нарушителю ИБ является его увольнение. Но увольнение может также являться мотивом для совершения преступления в виде ИТ-саботажа и кражи ИСб в целях получения деловых преимуществ в одиночку и с соучастниками.

Основные элементы системы поведения внутреннего нарушителя ИБ приведены в табл. 2, а схема их взаимодействия – на рис. 1.

Таблица 2

Основные элементы системы поведения внутреннего нарушителя ИБ

№	Элемент	Другие элементы, оказывающие на него воздействие
1	Мотивация инсайдера	Реакция организации Сговор Увольнение инсайдера
2	Реакция организации	Получение информации об инсайдере
3	Получение информации	Поведение инсайдера
4	Технические возможности инсайдера	Реакция организации Сговор Увольнение инсайдера Поведение инсайдера
5	Сговор	Мотивация инсайдера Технические возможности инсайдера
6	Ущерб организации	Поведение инсайдера
7	Увольнение инсайдера	Мотивация инсайдера Реакция организации
8	Поведение инсайдера	Мотивация инсайдера Технические возможности

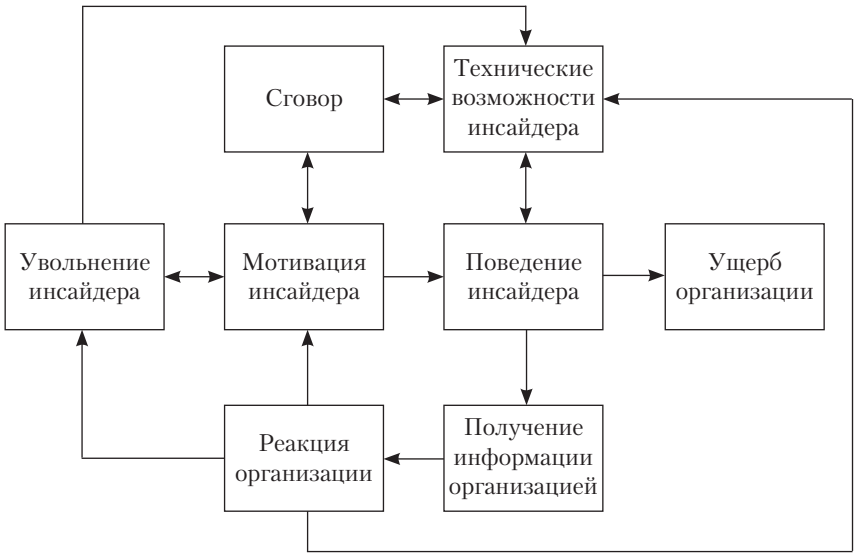


Рис. 1. Схема взаимодействия основных элементов системы поведения внутреннего нарушителя ИБ

Системно-динамическое моделирование кражи интеллектуальной собственности в целях получения деловых преимуществ в одиночку

На основе проанализированных исследований и информации об инцидентах, полученной из других открытых источников, разработан портрет внутреннего нарушителя для угрозы кражи ИСб в целях получения деловых преимуществ в одиночку, приведенный в табл. 3, и характерные особенности угрозы, приведенные в табл. 4.

Таблица 3

Портрет нарушителя
для кражи ИСб в одиночку

№	Характеристика	Описание
1	Занимаемая должность в организации	Разработчик ПО, научный сотрудник, менеджер по работе с клиентами, руководитель (преступники, как правило, занимают техническую позицию, но не являются привилегированными техническими пользователями)
2	Методы атаки	Технически простые, с использованием легально предоставленных прав и полномочий
3	Характер действий	Кража конфиденциальной информации, как правило, ИСб: ПО, секреты производства, бизнес-планы, базы клиентов, физическое оборудование
4	Длительность преступления	1 (реже 2 и больше) месяц до увольнения
5	Обнаружение преступления	Сообщение от клиентов Сообщение от коллег (занимающих, как правило, нетехнические позиции в организации) Внезапное появление конкурирующего предприятия Мониторинг ИБ и ИТ-аудит Системы обнаружения и предотвращения утечки информации

Таблица 4

Характерные особенности
кражи ИСб в одиночку

№	Характерная особенность	Элемент
1	Большая часть инсайдеров крадет информацию, связанную непосредственно с их работой, и зачастую участвует в разработке данной информации. По мере вовлеченности инсайдера в деятельность организации растут его вклад и чувство того, что он обладает правами на произведенный продукт, в особенности если он участвовал в процессе его разработки	Мотивация инсайдера
2	Для кражи ИСб в целях получения деловых преимуществ в одиночку зачастую характерна обида сотрудника на организацию	Мотивация инсайдера
3	Инсайдер, как правило, не проводит подготовки или планирования	Мотивация инсайдера
4	Большинство инсайдеров, осуществивших кражу ИСб в целях получения деловых преимуществ в одиночку, подписывали соглашение об ИСб. Напоминать о соглашении об ИСб и ответственности за кражу ИСб необходимо регулярно во время обучения ИБ	Мотивация инсайдера
5	Инсайдеры, как правило, не воспринимают кражу ИСб в целях получения деловых преимуществ в одиночку как преступление. Преступление совершается в половине случаев в течение месяца до увольнения, и инсайдер, как правило, не имеет четкого плана использования информации	Мотивация инсайдера Увольнение инсайдера Поведение инсайдера
6	Инсайдер действует в одиночку, может предпринять попытки скрыть следы	Поведение инсайдера Получение информации организацией
7	Признаками кражи ИСб в целях получения деловых преимуществ в одиночку могут являться передача большого объема информации во внешнюю сеть и/или на съемный носитель, а также внезапное появление конкурирующего предприятия.	Получение информации организацией

Окончание табл. 4

№	Характерная особенность	Элемент
	Информацию о потенциальном инциденте кражи ИСб в целях получения деловых преимуществ с соучастниками организация может получить от своих сотрудников, коллег или руководителей инсайдера, или от своих клиентов, которых инсайдер может пытаться использовать в своей деятельности	
8	Объемы кражи ИСб имеют тенденцию падать при получении инсайдером информации о подозрениях организации	Мотивация инсайдера Поведение инсайдера Получение информации организацией Реакция организации
9	Объемы кражи ИСб имеют тенденцию роста при заметании инсайдером следов своей деятельности	Мотивация инсайдера Получение информации организацией Поведение инсайдера

Для разработки ДПСС и ДП применялась среда моделирования Vensim, предназначенная для исследования сложных динамических систем, использовать которую можно бесплатно в научных целях. Обозначения, используемые в ДП и ДПСС в среде Vensim, пояснены в табл. 5.

Таблица 5

Обозначения, используемые в ДП и ДПСС

Внешний вид параметра	Пояснение
Уровень доступа, необходимый для получения информации	Переменная или константа
Желание совершить кражу	Уровень
Уменьшение желания совершить кражу	Поток, вызывающий изменение уровня
+	Положительная ПСС
-	Отрицательная ПСС
L	Логическая ПСС, неоднозначная зависимость, выражаемая в виде логической функции
<Желание совершить кражу>	«Призрачная» переменная. Вспомогательный элемент, являющийся ссылкой на переменную, указанную в треугольных скобках. Используется для упрощения внешнего вида ДП/ДПСС

ДПСС для угрозы кражи ИСб в целях получения деловых преимуществ с соучастниками представлена на рис. 2.

Рис. 2. ДПСС кражи ИСб в целях получения деловых преимуществ с соучастниками

По результатам анализа ДПСС следующие параметры диаграммы были выделены в качестве уровней: Вклад инсайдера в организацию, Желание совершить кражу, Чувство обладания правами на продукт, Осведомленность сотрудников о ИБ, Доверие организации к инсайдеру, Осведомленность организации о деятельности инсайдера.

ДП для кражи ИСб в целях получения деловых преимуществ в одиночку приведена на рис. 3.

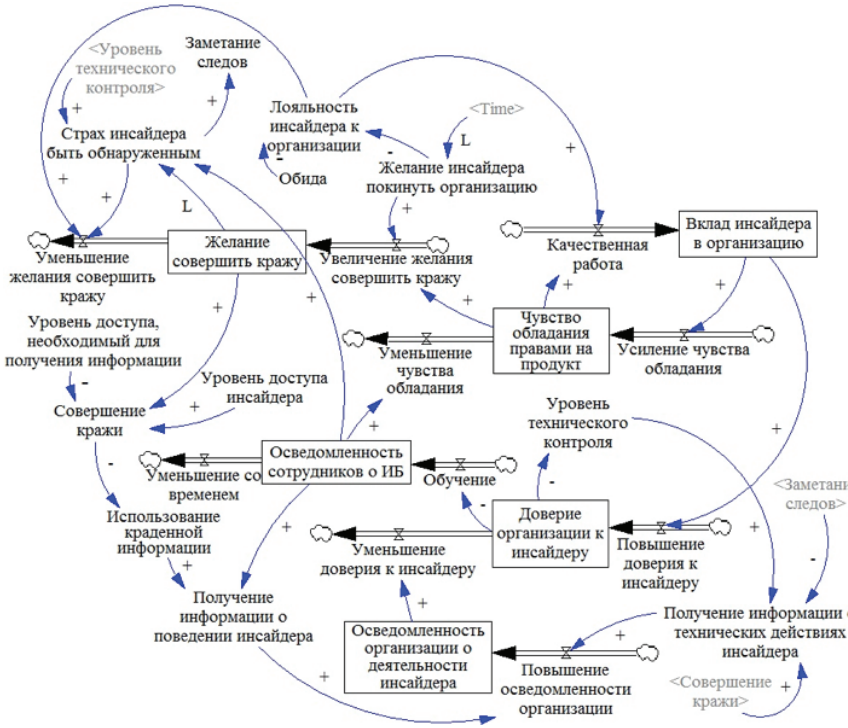


Рис. 3. ДП кражи ИСб в целях получения деловых преимуществ в одиночку

Проведем экспериментальное моделирование угрозы кражи ИСб в целях получения деловых преимуществ в одиночку. В первом эксперименте зададим низкое значение обиды инсайдера на организацию. Желание инсайдера покинуть организацию (возможно, сговор с конкурентом или начало своего предприятия) возникает на 30-й день моделируемой системы. Но несмотря на то что к 53-му дню эксперимента чувство обладания правами на разрабатываемый продукт достигает максимума, кража ИСб не была совершена ввиду высокой лояльности сотрудника (рис. 4).

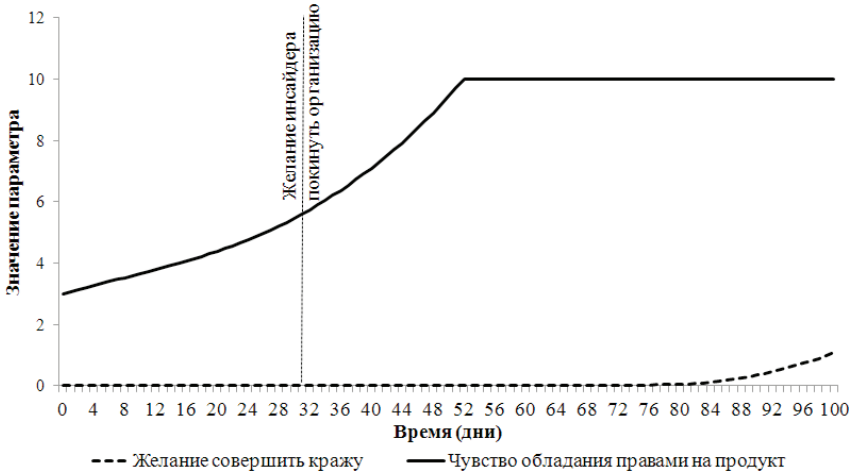


Рис. 4. Желание совершить кражу и чувство обладания правами на продукт при низком значении обиды инсайдера

Произведем моделирование повторно с изменением значения параметра обиды инсайдера на организацию на максимальный. В этом случае, несмотря на то что чувство обладания правами на производимый продукт не достигает своего максимума, кража ИСб совершается ввиду низкой лояльности инсайдера (рис. 5).

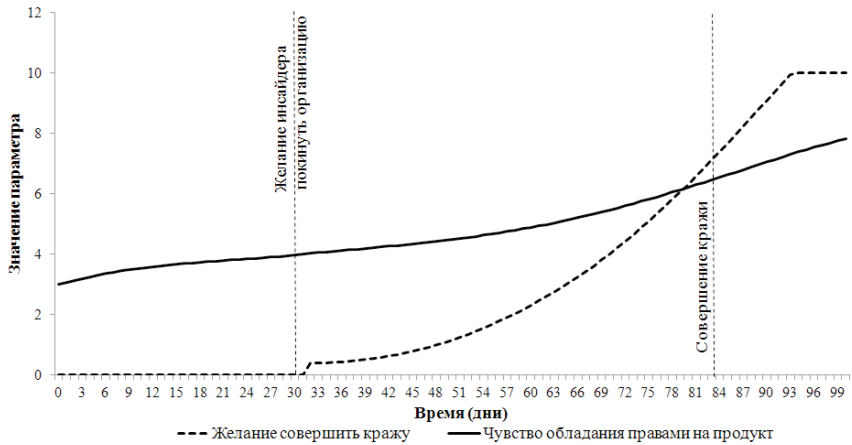


Рис. 5. Желание совершить кражу и чувство обладания правами на продукт при высоком значении обиды инсайдера

Системно-динамическое моделирование кражи интеллектуальной собственности в целях получения деловых преимуществ с соучастниками

На основе проанализированных исследований и информации об инцидентах, полученной из других открытых источников, разработан портрет внутреннего нарушителя для угрозы кражи ИСб в целях получения деловых преимуществ с соучастниками, приведенный в табл. 6, и характерные особенности угрозы, приведенные в табл. 7.

Таблица 6

Портрет нарушителя для кражи ИСб с соучастниками

№	Характеристика	Описание
1	Занимаемая должность в организации	Разработчик ПО, научный сотрудник, менеджер по работе с клиентами, руководитель. Зачастую инсайдеры занимают техническую позицию, но не являются привилегированными техническими пользователями
2	Методы атаки	У инсайдера не хватает полномочий, чтобы произвести кражу всего объема необходимой информации самому, поэтому ему приходится нанимать коллег
3	Характер действий	Кража конфиденциальной информации, как правило, ИСб: ПО, секреты производства, бизнес-планы, базы клиентов, физическое оборудование
4	Длительность преступления	1 (реже 2 и больше) месяц до увольнения
5	Обнаружение преступления	Сообщение от клиентов Сообщение от коллег (занимающих, как правило, нетехнические позиции в организации) Внезапное появление конкурирующего предприятия Мониторинг ИБ и ИТ-аудит Системы обнаружения и предотвращения утечки информации Информация об использовании украденной ИСб

Таблица 7

Характерные особенности кражи ИСб
с соучастниками

№	Характеристика	Элемент
1	Большая часть инсайдеров крадет информацию, связанную непосредственно с их работой, и зачастую участвует в разработке данной информации. По мере вовлеченности инсайдера в деятельность организации растет его вклад и чувство того, что он обладает правами на произведенный продукт, в особенности если он участвовал в процессе его разработки	Мотивация инсайдера
2	Для кражи ИСб в целях получения деловых преимуществ с соучастниками обида инсайдера на организацию нехарактерна	Мотивация инсайдера
3	Объемы кражи ИСб имеют тенденцию падать при получении инсайдером информации о подозрениях организации	Мотивация инсайдера Поведение инсайдера Получение информации организацией Реакция организации
4	Объемы кражи ИСб имеют тенденцию расти при заметании инсайдером следов своей деятельности	Мотивация инсайдера Получение информации организацией Поведение инсайдера
5	Объемы кражи ИСб имеют тенденцию падать ввиду долгого планирования, т. к. растет вероятность обнаружения организацией	Мотивация инсайдера Поведение инсайдера Получение информации организацией
6	Чем больше сил инсайдер инвестирует в планирование, тем сложнее ему отказаться от совершения преступления	Мотивация инсайдера
7	Если у инсайдера не хватает полномочий, он пытается привлечь других сотрудников. Перед наймом коллег инсайдер, как правило, производит попытки получения доступа самостоятельно	Сговор Поведение инсайдера

Окончание табл. 7

№	Характеристика	Элемент
8	Признаками кражи ИСб в целях получения деловых преимуществ с соучастниками может являться передача большого объема информации во внешнюю сеть и/или на съемный носитель, а также внезапное появление конкурирующего предприятия. Информацию о потенциальном инциденте кражи ИСб в целях получения деловых преимуществ с соучастниками организация может получить от своих сотрудников, коллег или руководителей инсайдера, или от своих клиентов, которых инсайдер может пытаться использовать в своей деятельности	Получение информации организацией
9	Большинство инсайдеров, осуществивших кражу ИСб в целях получения деловых преимуществ с соучастниками, подписывали соглашение об ИСб. Напоминать о соглашении об ИСб и ответственности за кражу ИСб необходимо регулярно во время обучения ИБ	Мотивация инсайдера

ДПСС для угрозы кражи ИСб в целях получения деловых преимуществ с соучастниками представлена на рис. 6.

По результатам анализа ДПСС следующие параметры диаграммы были выделены в качестве уровней: Вклад инсайдера в организацию, Желание совершить кражу, Чувство обладания правами на продукт, Вклад инсайдера в планирование, Осведомленность сотрудников о ИБ, Доверие организации к инсайдеру, Число привлеченных сотрудников, Осведомленность организации о деятельности инсайдера.

ДП для кражи ИСб в целях получения деловых преимуществ с соучастниками приведена на рис. 7.

Проведем экспериментальное моделирование с получением визуальной информации о поведении внутреннего нарушителя ИБ для угрозы кражи ИСб в целях получения деловых преимуществ с соучастниками. Желание инсайдера покинуть организацию и сговор с конкурентом (начало своего предприятия) возникают на 30-й день развития моделируемой системы, не-

удачная попытка получить доступ самостоятельно производится на 33-й день развития моделируемой системы, совершение кражи ИСб с привлечением соучастников происходит на 46-й день развития моделируемой системы. На рис. 8, 9 и 10 данные события изображены в виде функций-индикаторов (ступенек).

Рис. 6. ДПСС кражи ИСб в целях получения деловых преимуществ с соучастниками

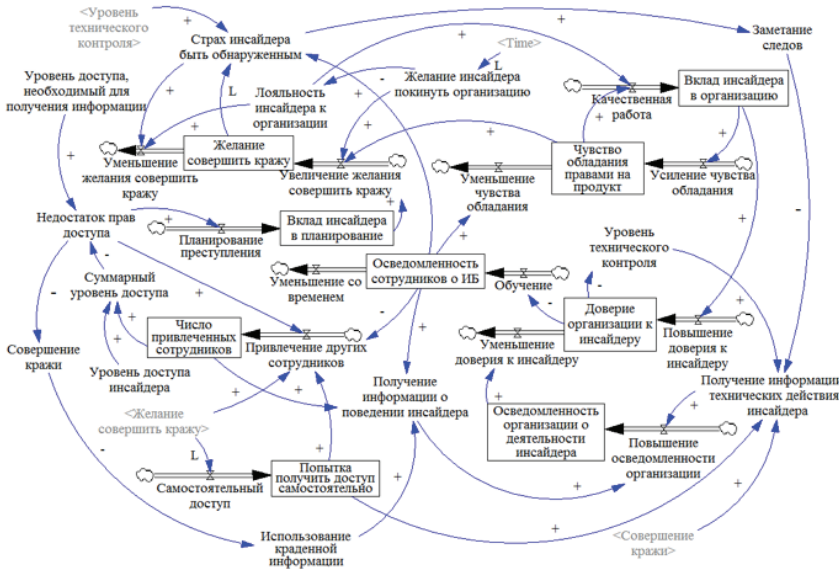


Рис. 7. ДП кражи ИСб в целях получения деловых преимуществ с соучастниками

Наем сотрудников изображен на рис. 8. В рамках эксперимента моделируемому инсайдеру удается привлечь трех соучастников для совершения кражи ИСб.

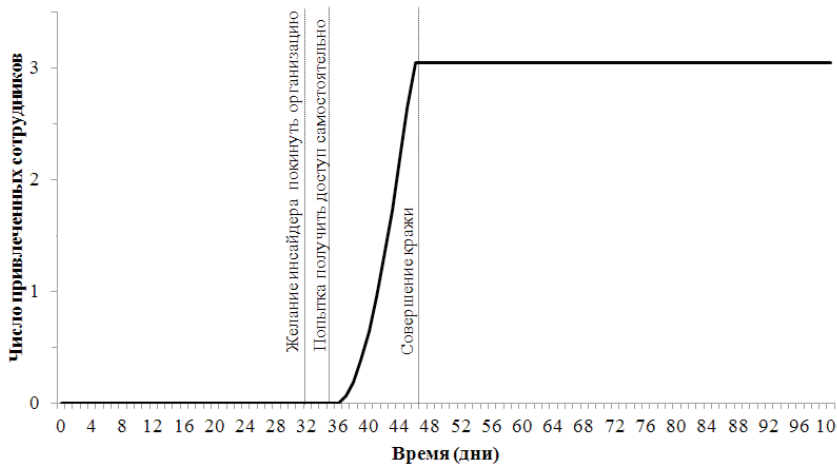


Рис. 8. Наем соучастников кражи ИСб

Доверие организации к инсайдеру первые 40 дней демонстрирует стабильный рост за счет хорошей работы до начала преступной деятельности, а осведомленность организации об инсайдерской деятельности достигает своего максимума через месяц после совершения кражи ввиду использования уволившимся инсайдером полученной информации в деятельности конкурирующего предприятия (рис. 9).

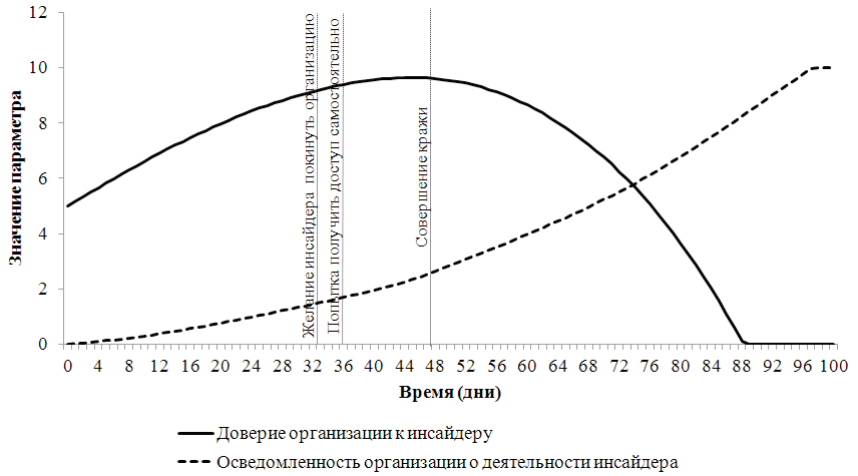


Рис. 9. Доверие организации к инсайдеру и осведомленность об инсайдерской деятельности

Это происходит ввиду большого изначального уровня доверия организации к инсайдеру, что вызывает недостаток технического контроля над действиями инсайдера и осведомленности сотрудников организации о ИБ (рис. 10).

Далее проведем тестовое моделирование с более низким начальным значением доверия к инсайдеру (4 вместо 5). В этом случае организации удается достаточно быстро обнаружить подозрительную деятельность инсайдера, повысить осведомленность о ИБ и уровень технического контроля, что помогает предотвратить совершение кражи (рис. 11).

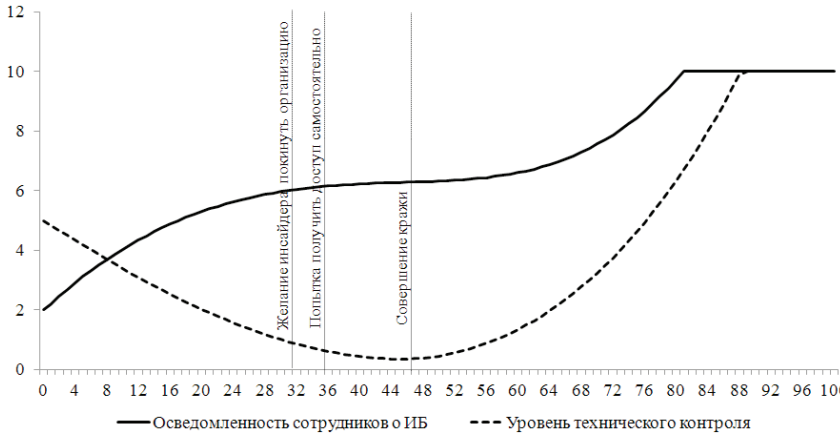


Рис. 10. Уровень технического контроля за инсайдером и осведомленность сотрудников о ИБ

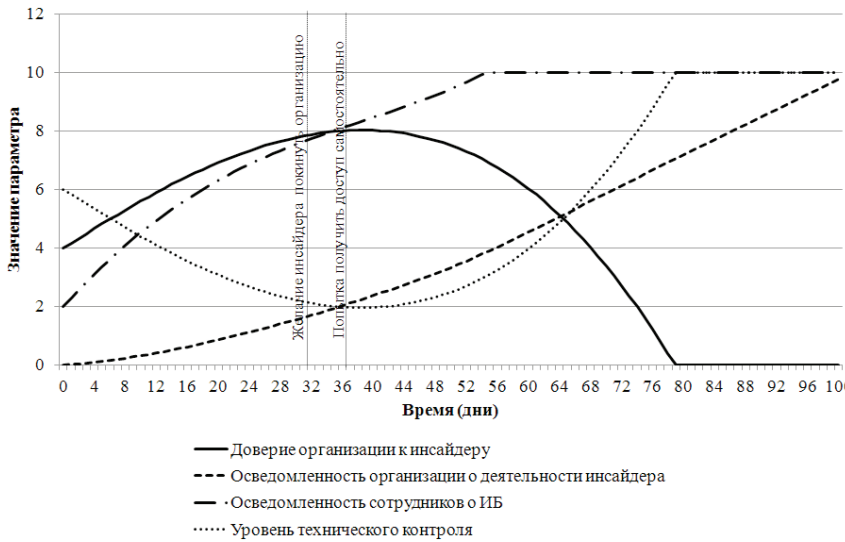


Рис. 11. Уменьшение начального значения показателя доверия организации к инсайдеру

Заключение

В данной статье представлен метод поддержки принятия решений по противодействию потенциальным внутренним нарушителям ИБ на основе системно-динамического моделирования поведения инсайдеров. Разработаны типовая структура модели внутреннего нарушителя ИБ и прогнозные системно-динамические модели кражи ИСб в целях получения деловых преимуществ. Проведено тестовое моделирование, подтверждающее адекватность полученных моделей.

Примечания

1 *Форрестер Дж.* Основы кибернетики предприятия. М.: Прогресс, 1971.

2 *Silowash G., Cappelli D., Moore A.P., Trzeciak R.F, Shimeall T.J., Flynn L.* Common Sense Guide to Mitigating Insider Treats. 4th ed. Software Engineering Institute. CERT Program, 2012.

3 *Зайцев А.С., Малюк А.А.* Исследование проблемы внутреннего нарушителя // Вестник РГГУ. 2012. № 14. Серия «Информатика. Защита информации. Математика». С. 114–134.

4 *Band S.R., Cappelli D.M., Moore A.P., Shaw E.D., Trzeciak R.F.* Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. Software Engineering Institute. CERT Program, 2006.

5 *Moore A.P., Cappelli D.M., Caron T.C., Shaw E., Trzeciak R.F.* Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model // First International Workshop on Manager Insider Security Threats (MIST 2009). Purdue University, West Lafayette, 2009.

6 *Cummings A., Lewellen T., McIntire D., Moore A.P., Trzeciak R.* Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector / Software Engineering Institute. CERT Program, 2012.

А.С. Рабинович

МЕТОД АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ С ИСПОЛЬЗОВАНИЕМ СЛУЖБЫ TSM В КАЧЕСТВЕ ДОВЕРЕННОГО ЭЛЕМЕНТА NFC-СИСТЕМЫ

В данной статье рассматривается метод интерактивной аутентификации пользователя с использованием службы TSM в качестве доверенного элемента NFC-системы.

В этом случае предлагается в состав существующих функций TSM-оператора, а именно функций гарантированного безопасного обмена данными и управления ключами для безопасного доступа к приложениям, добавить функцию управления ключами аутентификации пользователей NFC-системы как некоторый аналог функции управления сертификатами открытых ключей в PKI-инфраструктуре.

Ключевые слова: аутентификация пользователя, технология NFC, мобильный оператор, сертификат открытого ключа.

Введение

Технология беспроводной высокочастотной связи малого радиуса действия NFC (NFC[1]-технология) позволяет осуществлять бесконтактный обмен данными между устройствами, расположенными на небольших расстояниях. Модули NFC активно внедряются в разнообразные мобильные устройства – смартфоны, планшеты, ноутбуки – и могут использоваться для совершения покупок, оплаты проезда в общественном транспорте и других услуг, для удостоверения личности, в качестве электронного ключа от помещения или транспортного средства, а также для аутентификации пользователя и данных[2,3].

В данной работе предлагаются эффективные протоколы интерактивной аутентификации пользователей информационных

систем, построенных на основе NFC-технологии, с использованием службы TSM[4] (службы управления доверенными сервисами) в качестве третьей доверенной стороны. В качестве криптографической основы взяты параметры из схемы электронной подписи отечественного стандарта ГОСТ Р 34.10-2012.

Описание службы TSM, платформы OTA

Принцип существования единственного владельца ключей доступа входит в противоречие с вполне логичным желанием предоставлять пользователю услуги от нескольких независимых поставщиков. Такие сервис-провайдеры могут работать как на непересекающихся рынках (например, транспортная компания и банк), так и быть прямыми конкурентами. Но даже в первом случае компании, как правило, не желают предоставлять сторонним структурам доступ к своим данным. Подобное противоречие может быть решено как раз путем внедрения службы TSM – третьей стороны, которой доверяют все сервис-провайдеры.

Служба TSM – служба, которая позволяет поставщикам услуг и мобильным операторам управлять своими приложениями удаленно, обеспечивая доступ к защищенным элементам на терминалах с поддержкой NFC-технологии. Владелец TSM-сервера выступает в качестве посредника, который устанавливает деловые соглашения и технические связи между оператором мобильной связи, поставщиками услуг или другими лицами, контролирующими доступ к защищенным элементам бесконтактного приложения на мобильных терминалах с поддержкой NFC-технологии.

Для контроля над приложениями мобильный оператор устанавливает их на SIM-карту пользователя. SIM[5]-карта (модуль идентификации абонента) представляет собой идентификационный модуль абонента, применяемый в мобильной связи. Основная функция SIM-карты – хранение идентификационной информации об аккаунте (учетной записи абонента), что позволяет пользователю легко и быстро менять сотовые аппараты, не меняя при этом свой аккаунт, а просто переставив SIM-карту в другой телефон. Для этого SIM-карта включает в себя микропроцессор с программным обеспечением и данные с ключами идентификации карты, записываемые в карту на этапе ее производства, используемые на этапе идентификации и персонализации карты, например сетью GSM.

Область памяти на SIM-карте может эффективно использоваться и в качестве хранилища NFC-приложения. Сегодня обыч-

ный бумажник содержит большое количество пластиковых карт различных типов – банковские карты, дисконтные карты, билеты, членские карточки, пропуска, – все карты с магнитной полосой могут быть представлены в качестве NFC-приложений на SIM-карте. Преимуществом ее использования являются привязка карты к абоненту; совместимость между мобильными телефонами; собственная система безопасности. Области памяти смарт-карт представлены на рис. 1. При этом секретные и идентификационные параметры пользователя при эксплуатации новых схем защиты данных могут храниться в незадействованных областях SIM-карты (см. далее).

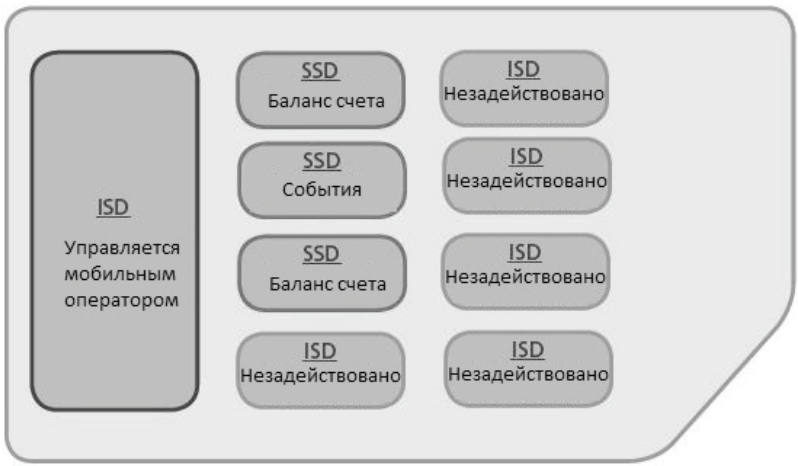


Рис. 1. Области памяти SIM-карты

Как и в любой среде приложений, возникает необходимость добавления новых приложений, удаление старых, обновление существующих новыми версиями и предоставление приложениям актуальных данных. Такая система управления требует использования платформы OTA[6]. Платформа OTA – это часть инфраструктуры оператора, обеспечивающая работу с SIM-картами по протоколам GSM 03.48 и 23.048 (единые стандарты для всех производителей). На базе данной платформы оператор может запустить большое число дополнительных сервисов.

NFC-приложение на SIM-карте может быть резидентным, но может возникнуть необходимость предоставления приложению

пользовательского интерфейса. Примеры приложений, которые требуют пользовательского интерфейса: активация приложения при покупке из торгового автомата (терминала), информация по дисконтным картам, перечень кредитных/дебетовых карт, доступных для использования, подтверждение ежемесячной покупки билета на транспорт.

В NFC-системе мобильный оператор сети предоставляет для хранения приложения, распространяемые среди абонентов SIM-карты. Таким образом, у оператора есть возможность выбрать соответствующую бизнес-модель и, следовательно, выбрать права персонализации, которые будут поддерживаться на стороне SIM-карты и которые будут доступны для его партнеров (поставщиков услуг и менеджеров службы).

Существует три основных сценария для различных бизнес-моделей[7]:

- простой режим (Simple Mode): эмитент-ориентированная модель, где управление содержимым SIM-карты выполняется только оператором, но контролируется TSM;
- режим доверенного управления (Delegated Mode): управление содержимым карты может быть делегировано TSM, но каждая операция требует авторизацию от оператора;
- режим авторизованного управления (Authorized Mode): управление содержимым SIM-карты полностью делегировано TSM.

На стороне мобильного оператора возможна реализация в двух вариантах:

- служба TSM реализуется самим оператором;
- служба TSM реализуется сторонними организациями.

В первом случае, при организации службы TSM на стороне оператора, передача данных по операции возможна как напрямую в терминал (телефон с поддержкой NFC-технологии), так и через платформу OTA. Платформу OTA предпочтительно использовать для балансировки нагрузки при передаче данных, тогда управление приложением происходит напрямую от службы TSM.

В случае же реализации службы TSM сторонними организациями передача данных по операции происходит через так называемую службу Business Enabler для возможности контроля операций со стороны оператора (см. рис. 2). Business Enabler позволяет мобильному оператору активировать или деактивировать службу TSM сторонних организаций. После успешного прохождения операции через службу Business Enabler дальнейшая передача данных возможна как напрямую в терминал, так и через платформу OTA.

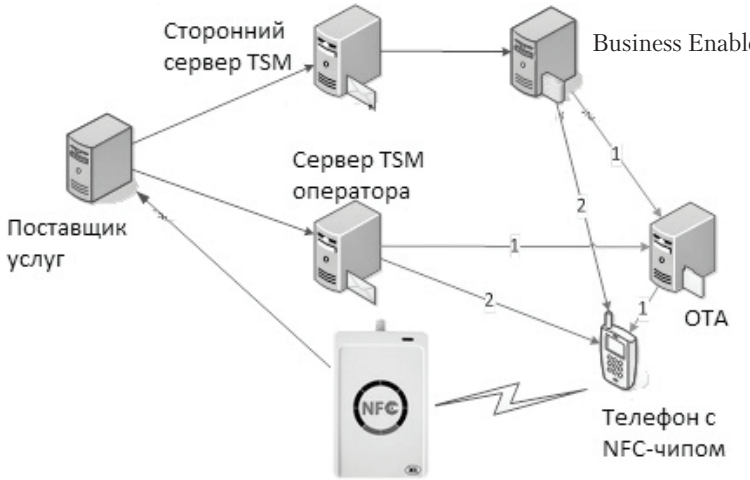


Рис. 2. Взаимодействие компонентов NFC-системы

Основные функции TSM-оператора:

- обеспечение связи между мобильным оператором и провайдером услуг;
- гарантия безопасного обмена данными;
- управление жизненным циклом бесконтактного приложения;
- загрузка и персонализация бесконтактного приложения посредством OTA;
- активация и деактивация услуг;
- обновление пользовательского интерфейса;
- управление клиентской базой данных NFC;
- обновление EMV-баланса (баланс карт Europay, MasterCard и VISA) для оплаты;
- управление услугами с добавленной стоимостью, такими как перерегистрация билета;
- управление ключами для безопасного доступа к приложению.

В случае использования TSM-оператора для решения задачи аутентификации пользователей NFC-системы в настоящей работе предлагается в состав функций гарантированного безопасного обмена данными и управления ключами для безопасного доступа к приложению добавить функцию (подфункцию) управления открытыми ключами аутентификации пользователей и их сертификатами (является аналогом функции управления сертификатами открытых ключей в PKI[8]-инфраструктуре).

Таким образом, в данной работе предлагается расширить возможности службы TSM – использовать службу для аутентификации пользователей в NFC-системах. В этом случае служба TSM будет хранить полную информацию о пользователе – от аутентификационных данных пользователя (ФИО, идентификационный номер или логин) до прав доступа, которыми обладает пользователь по отношению к ресурсам NFC-системы (см. рис. 3).

Рис. 3. Взаимодействие компонентов NFC-системы при использовании службы TSM для аутентификации пользователя в NFC-системе

При такой схеме NFC-система напрямую не доверяет пользователю. В случае запроса доступа к ресурсам будет создан запрос данных третьей доверенной стороне (службе TSM). Служба TSM, в свою очередь, посылает сообщение с данными пользователя NFC-системе, на основе которого уже предоставляется / не предоставляется запрошенный пользователем доступ.

Протокол интерактивной аутентификации

Схема интерактивной аутентификации, рассматриваемая в данной работе, позволяет обеспечить надежный доступ абонентов некоторой информационной системы к различного рода удаленным ресурсам. В таких системах субъект доступа **P** (доказывающий) гарантированно доказывает объекту доступа **V** (проверяющему) наличие у себя секретных реквизитов, не раскрывая никакой сколько-нибудь значимой информации об этих реквизитах. Данная

схема предусматривает наличие третьего необходимого доверенного элемента – центра доверия, который осуществляет основные управляющие функции по установлению защищенных соединений в системе. В нашем случае мы будем использовать в качестве такового TSM-оператор и именовать такой центр – центр управления ключами – **ЦУК**.

Описание схемы интерактивной аутентификации ***ИА***. Все криптографические соглашения в данной схеме можно найти в статье О.В. Казарина и А.Д. Сорокина[9]. Работа начинается с того, что **ЦУК** выбирает параметры, так же как и в схеме электронной подписи стандарта ГОСТ Р 34.10-2012, а именно абоненты **Р** и **V** заранее договариваются о совместном использовании следующих параметров: группы $E(0,b)/q^*$ с порядком $N_{q^*} = q+1$ и образующим G с длиной числа $|q^*| = 256$ битов.

Абонент системы **Р** (в данном случае в его качестве будет выступать *NFC-устройство*) «приходит» для регистрации в **ЦУК** и вместе с **ЦУК** выбирает секретный ключ $d : 0 < d > q$ и соответствующий ему открытый ключ как точку эллиптической кривой Q с координатами (x_Q, y_Q), такую, что $dG=Q$. Далее для этого абонента **ЦУК** составляет идентификационную строку I, состоящую из имени, адреса, уровня полномочий и т. п. Затем для Q и I генерируется электронная подпись **ЦУК** s. Схема подписи в данном случае может быть любой из известных. Абоненту выдаются подпись s, ключи d и Q, строка I и простое q^*. Секретный ключ d предлагается хранить в незадействованных ISD-областях SIM-карты (см. рис. 1).

Процесс интерактивной аутентификации, в котором абонент **Р** сначала будет доказывать, что s есть подписи **ЦУК**, а затем доказывать, что он имеет в наличии секретный ключ d абоненту **V** (в данном случае в его качестве будет выступать *устройство считывания данных с NFC-устройства РД*) без раскрытия самого секретного значения d, начинается с отсылки подписи s и значений (I, Q) абоненту **V**. Абонент **V** с помощью открытого ключа **ЦУК** верифицирует идентификационную строку I и открытый ключ Q абонента **Р**.

Ниже приводится протокол интерактивной аутентификации, «соответствующий» указанной выше схеме электронной подписи с очевидными сокращениями, которые «не теряют» общую идею построения протоколов подобного вида.

Протокол ИА

Интерактивная часть протокола выполняется в l циклах по i:

1. Абонент **P**: генерирует случайное целое число k_i: $0 < k > q$, вычисляет точку эллиптической кривой $C_i=k_iP$ и берет ее абсциссу: $r_i = [x_{Ci}](\mathrm{mod} q^*)$.

2. Абонент **V**: выбирает $e_i \in_R \{1,...,2^t\text{-}1\}$, где t – некоторый параметр безопасности, и выдает e_i абоненту **P**.

3. Абонент **P**: вычисляет $s_i \equiv [r_i d + k_i e_i](\mathrm{mod}\ N_{q^*})$ и отсылает s_i абоненту **V**.

4. Абонент **V**: вычисляет $v_i \equiv [e_i^{-1}](\mathrm{mod}\ N_{q^*})$, $z_{1i} \equiv [s_i v_i](\mathrm{mod}\ N_{q^*})$, $z_{2i} \equiv [-r_i v_i](\mathrm{mod}\ N_{q^*})$ и точку эллиптической кривой $C = z_{1i}P + z_{2i}Q$, берет ее абсциссу x_{Ci}, вычисляет $R_i \equiv [x_{Ci}](\mathrm{mod}\ q^*)$ и проверяет: $R_i \equiv r_i$. Если проверки на шаге 4 во всех l циклах завершены корректно, то процесс аутентификации абонента системы **P** завершен успешно, в противном случае абонент **V** «сигнализирует» о попытке несанкционированного доступа.

*Безопасность протокола **ИА***. Стойкость протокола **ИА** доказывается стандартным образом[10,11,12,13,14], когда доказываются следующие три утверждения.

1. Если абоненты **P** и **V** являются честными, тогда последний примет доказательства первого с вероятностью 1 (*свойство полноты протокола интерактивной аутентификации*).

2. Если абонент **P** – нечестный, не знает секретного ключа d (т. е. $\mathbf{P}^*$), то тогда, что бы ни предпринимал $\mathbf{P}^*$, он не сможет обмануть абонента **V** с вероятностью, близкой к 1 (*свойство корректности протокола интерактивной аутентификации*).

3. Если абонент **V** – нечестный (т. е. $\mathbf{V}^*$), то он не может получить никакой полезной для себя информации о значении d (*свойство нулевого разглашения* (*zero-knowledge*), или *свойство неразличимости свидетельств* (*witness indistinguishable*), или *свойство сокрытия свидетельства* (*witness hiding*) *протокола интерактивной аутентификации*).

Выбор аддитивной абелевой группы точек эллиптической кривой для реализации различных криптографических схем и протоколов, в том числе для схемы подписи стандарта ГОСТ Р 34.10-2012, обоснован тем, что ее структура является более богатой, чем традиционно используемая мультипликативная абелева группа вычетов конечного поля и тем самым криптографические параметры для различных протоколов можно выбирать более гибко. Тем более что при обеспечении одной и той же

криптографической стойкости протоколов вычисления в группе точек эллиптической кривой выполняются примерно на 20% быстрее, чем в указанной группе вычетов[15].

Для повышения быстродействия обмена данными при аутентификации предлагается искать, как всегда, разумный и обоснованный компромисс между криптографической стойкостью и эффективностью реализации за счет подбора подходящих значений длин секретных ключей, количества раундов схемы аутентификации и т. д. Это определяется, в конце концов, политикой безопасности того объекта (уровнем важности, критичности объекта), к которому осуществляется доступ, в том числе при помощи различных схем аутентификации субъекта доступа.

Заключение

Благодаря высокой скорости соединения и минимальному расстоянию между устройствами обеспечивается быстрая и безопасная передача данных, что особенно актуально при использовании NFC-устройства, синхронизированного с банковской картой. Особенно актуальной данная область применения технологии NFC стала с появлением смартфонов Samsung, HTC, BlackBerry, Nokia, Google со встроенными NFC-чипами и возможностью запуска различных бизнес-приложений.

Появление службы Trusted Service Manager для работы с приложениями позволит поставщикам услуг и мобильным операторам не только оптимизировать свои инвестиции в оборудование и ускорить реализацию проектов без каких-либо компромиссов в вопросах контроля над приложениями и данными, но и решать новые задачи защиты информации в NFC-системах, одна из которых и предлагается в настоящей работе.

Примечания

1 От англ. Near Field Communication.

2 *Рабинович А.С., Казарин О.В.* Методика аутентификации пользователя в информационной системе с использованием технологии NFC // Вопросы кибербезопасности. 2013. № 2. С. 59–62.

3 *Рабинович А.С., Казарин О.В.* Аутентификация пользователя информационной системы с использованием технологии NFC // Сб. тр. Междунар. науч.-практ. конф. «СИТ-2014». М.: Изд-во МФЮА, 2014. С. 53–57.

[4] От англ. Trusted Service Manager.

[5] От англ. Subscriber Identification Module.

[6] От англ. «Over The Air».

[7] *The European Payments Council and the GSM Association*. EPC – GSMA Trusted Service Management Requirements and Specifications, 2010.

[8] От англ. Public Key Infrastructure.

[9] *Казарин О.В., Сорокин А.Д.* Протоколы интерактивной идентификации, основанные на схеме электронной подписи ГОСТ Р 34.10-2012 // Вопросы защиты информации. 2014. № 2 (105). С. 43–50.

[10] *Brickell E.F., McCurley K.S.* Interactive identification and digital signatures // AT&T Technical Journal. Nov. / Dec. 1991. Vol. 70. № 6. P. 73–86.

[11] *Feige U., Fiat A., Shamir A.* Zero-knowledge proofs of identity // Journal of Cryptology. 1988. Vol. 1. № 2. P. 77–94.

[12] *Feige U., Shamir A.* Witness indistinguishable and witness hiding protocols // Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC). N. Y., 1990. P. 416–426.

[13] *Fiat A., Shamir A.* How to prove yourself: practical solutions to identification and signature problems // Lecture Notes in Computer Science. Advances in Cryptology – CRYPTO'86. 1987. Vol. 263. P. 186–194.

[14] *Schnorr C.P.* Efficient identification and signatures for smart cards // Lecture Notes in Computer Science. Advances in Cryptology – CRYPTO'89. 1990. Vol. 435. P. 239–252.

[15] *Miller S.* Uses of elliptic curves in cryptography // Lecture Notes in Computer Science. Advances in Cryptology – CRYPTO'85. 1986. Vol. 218. P. 417–426.

Ю.Д. Калинина

ФОРМИРОВАНИЕ ТЕХНИЧЕСКОГО КАНАЛА УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ В СЕТЯХ НА ОСНОВЕ ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЙ

В статье приводится описание существующих и применяемых в настоящие время сетей на основе волоконно-оптических технологий и дается определение, описание, а также способ формирования технического канала утечки речевой информации в сетях на основе волоконно-оптических технологий.

Ключевые слова: волоконно-оптические технологии, речевая информация, технические каналы утечки.

Волоконно-оптические коммуникации (ВОК) на сегодняшний день являются наиболее перспективным направлением проводных систем связи с уверенной линией развития. В связи с широкой распространенностью актуализируется проблема защиты информации в таких системах. Долгое время оптическому волокну приписывалась повышенная скрытность из-за таких достоинств волокна, как широкополосность и малые потери. В строительстве внутригородских сетей связи наряду с этими свойствами особое значение приобретают малый диаметр и отсутствие взаимной интерференции, а в электрически неблагоприятной окружающей среде – безындукционность. Большое значение имеет и высокая степень защищенности от несанкционированного съема информации по сравнению с электромагнитным и волноводными каналами связи на меньшей несущей частоте, что определяется особенностями распространения излучения по оптическим волокнам и трудностями скрытного подсоединения к существующим линиям. Физико-технические принципы, на которых возможно формирование каналов утечки различного

вида информации, изменяются полностью. Оптическое излучение сильно поглощается в естественных природных материалах, так что становится практически невозможным дистанционный съем информации. Несмотря на вышеперечисленные преимущества, утечка информации через волоконно-оптический кабель возможна. Невозможно защититься от неизвестного, поэтому в статье рассматривается технический канал утечки речевой информации в сетях на основе волоконно-оптических технологий. В настоящее время существуют разные технологии построения оптических сетей.

Волоконно-оптические технологии

Технология PON (Passive optical network, пассивная оптическая сеть) является распределенной сетью доступа, основанной на волоконно-кабельной древовидной архитектуре с пассивными оптическими разветвителями на узлах. Технология PON – это экономичный способ обеспечения широкополосной передачи информации, архитектура имеет высокую эффективность наращивания узлов и пропускной способности.

Главная особенность архитектуры PON заключается в использовании для передачи информации множества абонентских устройств ONT (optical network terminal) одного приемопередаточного модуля OLT (optical line terminal) в центральном офисе. Количество абонентских узлов, которые можно подключить к одному приемопередаточному модулю, зависит только от мощности и максимальной скорости приемопередаточной аппаратуры.

Технология FTTx (Fiber To The X, оптическое волокно до точки X) формально описывает только физический уровень, но в реальности включает значительное число технологий канального и сетевого уровня. Термин применим к любой телекоммуникационной сети, в которой оптоволоконный кабель от узла связи доходит до определенного места (точка X), а от точки X до абонента идет медный кабель.

Семейство FTTx представляют разные виды архитектур: волокно до сетевого узла, FTTN (Fiber to the Node); волокно до микрорайона, квартала или группы домов FTTC (Fiber to the Curb); волокно до здания FTTB (Fiber to the Building); волокно до жилища (квартиры или отдельного коттеджа) FTTH (Fiber to the Home). Основное различие архитектур – это расстояние от оптического кабеля до пользовательского терминала.

Структурированная кабельная система (СКС) – это иерархическая кабельная система, состоящая из структурных подсистем. Система позволяет объединить множество сетевых информационных сервисов, имеющих разное назначение: локальные телефонные и вычислительные сети, системы видеонаблюдения и безопасности и др. Ее оборудование состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток, а также из вспомогательного оборудования. Все элементы СКС интегрируются в единый комплекс (систему) и эксплуатируются согласно определенным правилам. Обычно элементы СКС помещают в кабель-канал, используя звукоизоляционные материалы.

Структуру кабельной системы определяет инфраструктура информационных технологий IT (Information Technology), именно она диктует содержание конкретного проекта кабельной системы в соответствии с требованиями конечного пользователя, независимо от активного оборудования, которое может применяться впоследствии.

Кроме телекоммуникационных применений, становление и развитие волоконно-оптических технологий открыло широкие возможности применения в приборостроении и измерительной технике. Почти одновременно с созданием волокон с малыми потерями появились работы по созданию волоконно-оптических датчиков физических величин. Современные волоконно-оптические датчики позволяют измерять практически все физические величины. К примеру, позволяют измерить давление, расстояние, положение в пространстве, скорость и угол вращения, электрический ток, напряженность магнитного поля, температуру, дозу радиационного излучения, скорость потока и давления крови, силу растяжения, изгиб, параметры звуковых волн и т. д. В частности, возможна регистрация воздействия на одномодовые и многомодовые световоды[1,2] звуковых и ультразвуковых колебаний.

Описание технического канала утечки информации в ВОК

Технический канал утечки информации (ТКУИ) является совокупностью объекта защиты (источника конфиденциальной информации), физической среды и технических средств разведки (ТСР) (промышленного шпионажа), которым добываются разведывательные данные[3].

ТКУИ в ВОК структурно представляет собой незначительно измененную стандартную модель ТКУИ. Источник конфиденциальной информации, в качестве которого выступает акустический сигнал (например, человек или аудиовоспроизводящие устройства и т. д.), преобразуется в сигнал, удобный для передачи, посредством модуляции света в оптическом волокне, в нашем случае роль передатчика выполняют паразитные модуляции и наводки в элементах ВОК. Информативный сигнал в виде модулированного оптического излучения в среде распространения информации, роль которой играют также ВОК, точнее, оптическое волокно, из которого они изготавливаются, распространяется далеко за пределы объекта защиты. Информативный сигнал выводится из оптического кабеля и попадает на приемник информации – демодулятор, преобразующий сигнал в форму, удобную для восприятия человеком. В качестве приемника используется фотоприемное устройство на основе фотодиода, преобразующее модулированный световой поток в электрический сигнал, который выводится в акустическую систему. В описываемой структуре ТКУИ приемник является техническим средством разведки (ТСР). Шумы в канале утечки формируются при воздействии внешних шумовых сигналов на среду распространения, модулятор и демодулятор сигнала и составляют аддитивный шум. Мультипликативная составляющая шума канала утечки через ВОК вносится приемником информации, т. е. связана с внутренними шумами системы регистрации. На последнем этапе преобразованный сигнал поступает к адресату или злоумышленнику, как показано на рис. 1.

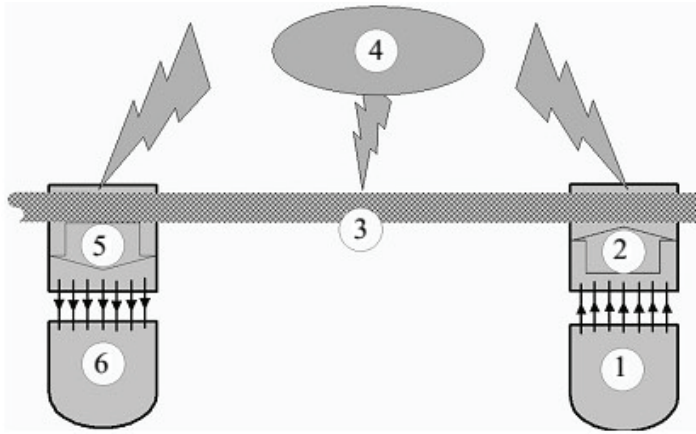


Рис. 1. Типовая структура обобщенного канала утечки информации:
1 – источник информации; 2 – передатчик; 3 – канал связи;
4 – шумы; 5 – приемник; 6 – адресат

Шумы технического канала утечки информации формируются главным образом на трех участках: при модуляции информативным сигналом световых потоков, при прохождении модулированного светового сигнала по каналу связи и при демодуляции информативного сигнала техническими средствами разведки. Если исходный сигнал обладал отношением SNR_{in}, то на выходе канала утечки данное отношение уменьшается до SNR_{out} в CNL в дБ, являющийся коэффициентом шума, общая величина которого выражается как

$$CNL = CNL_m + CNL_d + CNL_r,$$

где CNL_m – шумы при модуляции, CNL_d – шумы канала связи, CNL_r – шумы при демодуляции. В ТКУИ через ВОК шумы, наводимые при распространении света по оптическим волокнам, незначительны, т. е.

$$CNL_d \approx 0,$$

поэтому общий коэффициент шума CNL определяется исключительно шумами при модуляции CNL_m и при демодуляции CNL_r.

Выбор ТСР непосредственно зависит от типа и параметров канала утечки. Для ВОК выделяют три типа каналов утечки, связанные с наиболее уязвимыми местами линий связи. Применение ТСР в отношении данных каналов утечки особенно актуально.

1. Канал утечки типа А: связан с разрывными соединениями кабеля, включает разъемные и неразъемные соединения.

2. Канал утечки типа В: определяется конструктивными особенностями свободного волоконно-оптического кабеля.

3. Канал утечки типа С: вызван особенностями монтажа кабеля при креплении к конструкциям здания; вспомогательные элементы (короба, лотки) повышают чувствительность волокна к виброакустическим колебаниям[4].

Основным параметром по оценке эффективности канала утечки информации может быть принята глубина модуляции

$$CML = \frac{\delta P}{P_0},$$

где δP – амплитуда модуляции мощности оптического излучения, P_0 – мощность оптической несущей. Так как глубина модуляции непосредственно связана с уровнем звукового давления информативного сигнала на входе канала утечки, то подобное предположение является естественным. Чем выше уровень звукового давления, тем больше глубина модуляции и тем эффективнее канал утечки.

Формирование ТКУИ в ВОК

Волоконно-оптические коммуникации применяются повсеместно и выполняют функции как передачи, так и сбора информации. Эта многогранность применения обусловлена высокой чувствительностью элементов ВОК к изменениям в окружающей среде.

Основные физические принципы формирования каналов утечки речевой информации через волоконно-оптические коммуникации связаны с воздействием акустического поля на пассивные элементы и конструктивные части волоконно-оптического кабеля. Такое воздействие приводит к паразитным модуляциям и наводкам в оптическом излучении.

При воздействии звука на оптический кабель, по которому распространяется свет, происходит изменение оптической длины пути света, что приводит к изменению фазы световой волны. Это

изменение фазы может быть зарегистрировано обычными интерферометрическими методами. В общем случае звуковое поле оказывает сложное воздействие на световую волну, вызывая ее амплитудную, поляризационную, частотную и фазовую модуляции. Подобное воздействие звук оказывает на любую среду, в том числе и на остальные элементы волоконно-оптической сети. Величина модуляции обычно пропорциональна длине акустооптического взаимодействия и звуковому давлению. Паразитные модуляции светового потока могут быть сняты при наличии определенной аппаратуры. Вопрос уменьшения влияния акустического воздействия на оптический кабель решается путем его звукоизоляции, однако полностью оградить волокно от внешнего воздействия звука достаточно сложно.

Эффекты модуляции светового потока звуковым акустическим сигналом частично связаны с типом волокна[5], частично с конструкцией кабеля и с техникой монтажа, так как оптоволокно чувствительно к механическим деформациям.

Коэффициент модуляции канала утечки (CML) определяется в зависимости от вида несущего поля и модулируемого параметра. Коэффициент модуляции является характеристикой конкретного преобразования и определяет долю информационного сигнала от амплитуды несущего. Отличительной особенностью является то, что его величина в канале утечки имеет значение намного меньшее единицы. Это естественное приближение, связанное с тем, что модуляция является паразитным эффектом, которое стремятся максимально ослабить. Практические методы определения коэффициента модуляции связаны с экспериментальным измерением коэффициента (глубины) модуляции несущего поля внешним информационным полем в зависимости от величины внешнего воздействия[6].

В качестве основного механизма формирования модулированного сигнала будем считать несогласованность в месте разъемного соединения (рис. 2). Механическое торцевое соединение двух волокон приводит к оптическим потерям в виде обратного френелевского отражения, на основе которого возможно формирование утечки.

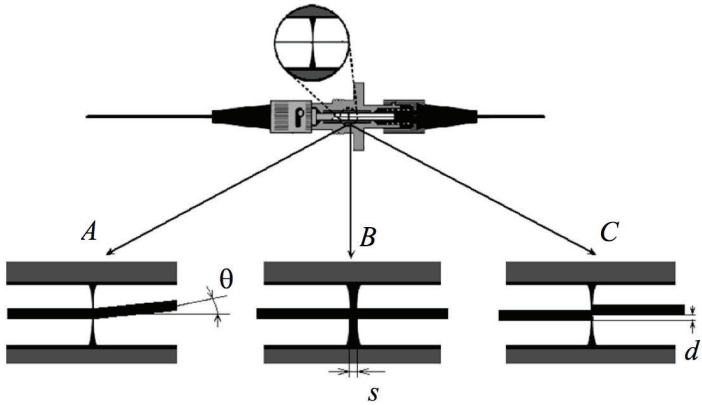


Рис. 2. Схематическое изображение разъемного соединения с неточностью соединения.
A – угловое рассогласование с углом Θ;
B – неплотное соединение с расстоянием между волокнами *s*;
C – радиальное смещение на расстояние *d*.

Величина потерь для современных разъемов составляет порядка 0,75 дБ[7]. В зависимости от вида рассогласования величина потерь варьируется и дается выражениями[8]:

$$\alpha_{\Theta} = 10 \cdot lg\left(1 - \frac{2n_0}{NA} \cdot \frac{\Theta}{\pi}\right)$$

для углового рассогласования на угол *Θ*;

$$\alpha_s = 10 \cdot lg\left(1 + \frac{S}{a} \cdot \mathrm{ta_n}\left[\frac{\arcsin NA}{n_0}\right]\right)$$

для неплотного соединения волокон с промежутком *s*;

$$\alpha_d = 10 \cdot lg\left(1 - \frac{2}{\pi} \cdot \frac{d}{a}\right)$$

для радиального смещения между ступенчатыми волокнами на расстояние *d*[9].

Здесь введены обозначения: a – диаметр сердцевины оптического волокна; n_0 – показатель преломления иммерсионного слоя в стыке между волокнами; NA – числовая апертура волокна.

При воздействии звука геометрические параметры соединения Θ, s, d изменяются в зависимости от уровня звукового давления, что вызывает модуляцию отраженного и проходящего света. Оценим величину коэффициента модуляции канала утечки CML. В зависимости от вида разъема, материала и других параметров каждый из механизмов будет давать различные вклады. Во-первых, имеем модуляцию интенсивности света при радиальном смещении внутри соединения, для которого

$$CML_d = \frac{2}{\pi} \cdot \frac{\delta d}{a},$$

здесь δd – изменение радиального смещения между волокнами при воздействии акустического поля.

Второй вклад в модуляцию света в волноводе по порядку величины, близкий к CML_d, будет давать механизм, связанный с неплотным соединением, определяемый выражением

$$CML_s = \frac{\delta S}{a} \cdot \operatorname{ta}_{\mathrm{n}} \left[\frac{\arcsin NA}{\mathrm{n}_{\mathrm{o}}} \right].$$

Представленные выше два механизма модуляции дают наибольший вклад для одномодовых разъемных соединений, что связано с обратной зависимостью коэффициентов CML_d и CML_s от диаметра сердцевины волокна a, которая для многомодового волокна на порядок выше, чем для одномодового. Если принять для одномодовых соединений максимальное смещение вдоль или перпендикулярно оси волокна по порядку величины равным 0,05 мкм, то коэффициент модуляции может достигать 1% в обоих случаях. Вклад угловых рассогласований присутствует в обоих случаях, он определяется упругими свойствами материала и геометрическими размерами фиксирующей соединение втулки. Его величина определяется выражением

$$CML_\Theta = \frac{2\mathrm{n}_0}{NA} - \frac{\delta\Theta}{\pi}.$$

Формирование акустического информативного сигнала в канале утечки информации во многом зависит от уровня звукового

давления от источника информации и уровня шумов. Как правило, при переговорах уровень звукового давления речи намного превышает уровень шумов, если отсутствует акустическое зашумление. Поэтому уровень звукового давления является основным параметром оценки качества формирования информативного сигнала, чем выше уровень давления, тем эффективней модуляции и наводки.

Заключение

Волоконно-оптические технологии почти полностью захватили господство в области стационарных систем передачи благодаря своим характеристикам по скорости передачи, затуханию, а следовательно, по расстояниям, на которые возможна передача информации. Все больше инсталляций на волоконно-оптических кабелях находят применение в проектах, где раньше использовались медные. Это обусловлено многими факторами. Во-первых, ВОК имеют значительное преимущество перед проводными и радиоканалами в показателях пропускной способности, длины участка регенерации и помехозащищенности. Во-вторых, волоконно-оптический кабель имеет меньшие габариты и массу. И в-третьих, производство и монтирование волоконно-оптических линий связи становится относительно дешевле. Вопрос оценки акустического воздействия на оптический кабель требует должного внимания ввиду возможности формирования канала утечки речевой информации в помещениях, через которые он проходит.

Примечания

1 *Гуляев Ю.В., Меш М.Я., Проклов В.В.* Модуляционные эффекты в волоконно-оптических световодах и их применение. М.: Радио и связь, 1991. 152 с.

2 *Кульчин Ю.Н.* Распределенные волоконно-оптические измерительные системы. М.: Физматлит, 2001. 272 с.

3 *Халяпин Д.Б.* Защита информации. Вас подслушивают? Защищайтесь. М.: Гелиос АРВ, 2005. 960 с.

4 *Гришачев В.В., Халяпин Д.Б., Шевченко Н.А.* Волоконно-оптический телефон в акустооптоволоконном канале утечки конфиденциальной речевой информации // Вопросы защиты информации. 2009. № 3. С. 22–30.

5 Волоконно-оптические датчики / Под ред. Т. Окоси; пер. с яп. Г.Н. Горбунова. Л.: Энергоатомиздат, 1991. 255 с.

[6] *Гришачев В.В., Косенко О.А.* Практическая оценка эффективности канала утечки акустической (речевой) информации через волоконно-оптические коммуникации // Вопросы защиты информации. 2010. № 2. С. 18–25.

[7] *Листвин А.В., Листвин В.Н.* Рефлектометрия оптических волокон. М.: ВЭЛКОМ, 2005. 208 с.

[8] *Калинин В.А., Пресленев Л.Н.* Оптические волокна и пассивные компоненты волоконно-оптических линий связи: Учеб. пособие. СПб.: ГУАП, 2008. 80 с.

[9] *Гришачев В.В., Косенко О.А.* Количественная оценка эффективности канала утечки информации по техническим параметрам каналов связи // Вопросы защиты информации. 2010. № 4. С. 9–17.

В.И. Лобастов

ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ПЕРЕГОВОРОВ В САЛОНЕ АВТОМОБИЛЯ С ИСПОЛЬЗОВАНИЕМ ВИБРОАКУСТИЧЕСКИХ ИЗЛУЧАТЕЛЕЙ

В статье проанализированы основные недостатки известных методов активной защиты конфиденциальных переговоров в салоне автомобиля и предложен новый перспективный метод защиты с использованием виброакустических излучателей. В публикации представлены описание предложенного перспективного метода, принцип работы и две схемы его реализации. Кроме того, для оценки эффективности применения предложенного метода в статье представлены результаты экспериментов, проведенных при использовании специальной аппаратуры перехвата акустической информации в условиях имитации проведения конфиденциальных переговоров в салоне автомобиля с защитой переговоров предложенным методом.

Ключевые слова: защита акустической информации, акустическая защита, защита конфиденциальных переговоров в автомобиле, система защиты переговоров.

На сегодняшний день человеческая речь является наиболее естественным и распространенным способом обмена информацией между людьми. Защита акустической информации, которая зачастую является предметом перехвата, становится одним из важнейших аспектов комплексной защиты информации в эпоху становления и бурного развития постиндустриального общества. Высокие жизненные ритмы и удаленность специалистов практически всех сфер деятельности, их мобильность заставляют последних использовать автомобили для передвижения в различные точки хранения, обработки и передачи информации. В то же время излишняя мобильность и недостаток времени делают проблематичным быстрый и безопасный обмен речевой информацией по при-

чине отсутствия акустически изолированных помещений в месте проведения переговоров. Поэтому все чаще и чаще салон автомобиля используется для проведения конфиденциальных переговоров.

Известные на сегодняшний момент методы активной защиты конфиденциальных переговоров в салоне автомобиля (выполненные в виде отдельных устройств) требуют отдельной достаточно сложной настройки системы по необходимому уровню зашумляющего сигнала, выбора положения зашумляющей системы в салоне автомобиля, применения дополнительных устройств для обеспечения качества переговоров, отличаются относительно высокой себестоимостью.

Проведенные исследования показывают, что:

– установка не предусмотренных конструкцией салона автономных приборов (типа «Хаос-N», «Эхо-Кейс», «Шаман») с несколькими источниками шумовых сигналов (в том числе с мультимедийными колонками) может привести к интерференции их источников шума и созданию в ряде точек салона автомобиля устойчивой во времени ослабленной амплитуды результирующего сигнала, не обеспечивающей требуемого уровня защиты;
– место установки системы критично, и при изменениях в положении генератора в салоне автомобиля величина зашумляющей помехи может изменяться.

Указанные недостатки могут серьезно влиять на эффективность использования этих систем для защиты конфиденциальных переговоров в салоне автомобиля.

В настоящей статье для защиты конфиденциальных переговоров в салоне автомобиля рассмотрен следующий метод защиты, нивелирующий вышеуказанные недостатки: *зашумляющий сигнал подается на несущие конструкции автомобиля с помощью виброакустических излучателей, установленных на разведоопасных конструктивных элементах автомобиля.*

Предложенный метод защиты предлагается реализовывать в виде двух систем:

1. Системы, в которой зашумляющий сигнал подается на несущие конструкции автомобиля с помощью виброакустических излучателей со встроенным генератором помехи, установленных на разведоопасных конструктивных элементах автомобиля и подключенных к собственной автомобильной системе питания (Система защиты № 1)[1].

2. Системы, в которой зашумляющий сигнал подается на несущие конструкции автомобиля с помощью виброакустических

излучателей, установленных на разведоопасных конструктивных элементах автомобиля с использованием в качестве генератора зашумляющего сигнала собственной звуковой системы автомобиля (Система защиты № 2)[2].

Анализ наиболее разведоопасных направлений в автомобиле и ее архитектуры показал, что лобовое стекло, боковые стекла, заднее стекло являются самыми уязвимыми элементами с точки зрения акустической защищенности. Следующими по возможной угрозе возникновения виброакустического канала утечки информации являются капот, боковые двери. Исходя из этого, были выбраны следующие контрольные точки при проведении измерений.

Таблица 1

Контрольные точки

Номер контрольной точки	Описание контрольной точки
1	Лобовое стекло
2	Боковое стекло (переднее)
3	Заднее стекло
4	Капот
5	Боковая дверь (передняя)
6	Боковая дверь (задняя)

Для оценки эффективности Системы защиты № 1 проведены нижеперечисленные действия.

В соответствии с методикой слухового контроля путем измерения словесной разборчивости был проведен анализ защищенности салона автомобиля «Nissan Almera Classic» при использовании метода маскировки информативного сигнала шумовой помехой. Для проведения измерений использовался многофункциональный прибор ST031 «Пиранья», предназначенный для обнаружения и локализации специальных технических средств негласного получения информации, а также для решения ряда других задач защиты информации и контроля качества ее осуществления.

Акустический излучатель, имитирующий проведение конфиденциальных переговоров, устанавливался на заднем сидении салона автомобиля. Уровень излучения акустического излучателя составлял 75 Дб. В качестве имитирующего переговоры сигнала использовался тест Покровского.

Виброакустические излучатели со встроенным генератором помех, подключенные к бортовой системе питания автомобиля, крепились на конструкционные элементы автомобиля в соответствии с расположением контрольных точек. В качестве виброакустического излучателя со встроенным генератором помех использовался генератор-виброизлучатель «Соната-СП-45М».

На приемной стороне в контрольных точках устанавливался виброакустический датчик попеременно в каждой. Виброакустический датчик подключался к многофункциональному поисковому прибору ST031 «Пиранья». «Пиранья» использовался в режиме виброакустического преобразователя, к нему же подключались наушники. Аудитор в реальном времени записывал отдельные слова услышанного теста. После чего производилась обработка полученных результатов. Структурная схема экспериментальной установки представлена на рис. 1.

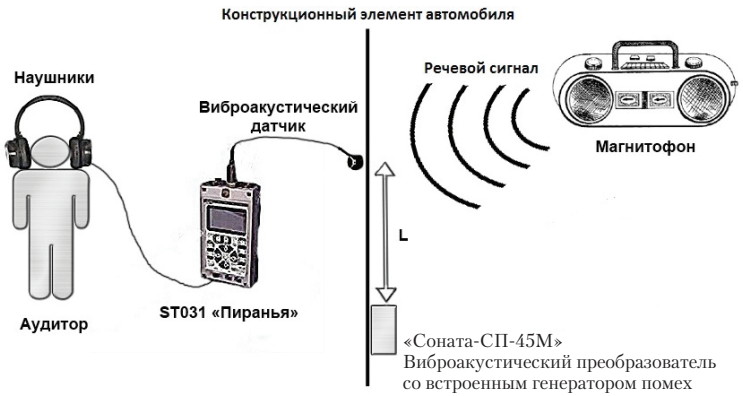


Рис. 1. Структурная схема экспериментальной установки

В процессе проведения анализа защищенности салона была определена зависимость дальности установки виброакустического излучателя со встроенным генератором помех от виброакустического датчика на словесную разборчивость переговоров, производимых в автомобиле.

Были выбраны три точки возможной установки виброакустического излучателя со встроенным генератором помех при неизменной позиции виброакустического датчика. Позиция 1: расстояние «Соната-СП-45М» – виброакустический датчик – 10 см; позиция 2: расстояние «Соната-СП-45М» – виброакустический

датчик – 40 см; позиция 3: расстояние «Соната-СП-45М» – виброакустический датчик – 80 см.

Для проверки степени защищенности речевого сигнала использовался метод речевой разборчивости (по W). При условии использования рассматриваемого метода защиты определялось количество правильно перехваченных слов в передаваемом тесте Покровского.

Практические опыты показывают, что составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 60–70%, краткой справки-аннотации – при словесной разборчивости менее 40–50%. При словесной разборчивости менее 20–30% значительно затруднено установление даже предмета ведущегося разговора, а при словесной разборчивости менее 10 % это практически невозможно[3].

Таблица 2

Речевая разборчивость
при использовании предлагаемой Системы защиты № 1

Номер контрольной точки	Название контрольной точки	Количество правильно принятых слов	Словесная разборчивость в %
Расстояние 10 см			
1	Лобовое стекло	0	0
2	Боковое стекло (переднее)	0	0
3	Заднее стекло	0	0
4	Капот	0	0
5	Боковая дверь (передняя)	0	0
6	Боковая дверь (задняя)	0	0
Расстояние 40 см			
1	Лобовое стекло	5	10
2	Боковое стекло (переднее)	4	8
3	Заднее стекло	0	0
4	Капот	0	0
5	Боковая дверь (передняя)	0	0
6	Боковая дверь (задняя)	0	0

Окончание табл. 2

Номер контрольной точки	Название контрольной точки	Количество правильно принятых слов	Словесная разборчивость в %
Расстояние 80 см			
1	Лобовое стекло	15	30
2	Боковое стекло (переднее)	–	–
3	Заднее стекло	12	24
4	Капот	9	18
5	Боковая дверь (передняя)	11	22
6	Боковая дверь (задняя)	5	10

Для оценки эффективности Системы защиты № 2 проведены нижеперечисленные действия.

В соответствии с методикой слухового контроля путем измерения словесной разборчивости был проведен анализ защищенности салона автомобиля Nissan Almera Classic при использовании метода маскировки информативного сигнала шумовой «речеподобной» помехой «речевой хор». Для проведения измерений использовался многофункциональный прибор компании «Смерш Технике» ST031 «Пиранья», предназначенный для обнаружения и локализации специальных технических средств негласного получения информации, а также для решения ряда других задач защиты информации и контроля качества ее осуществления.

Акустический излучатель, имитирующий проведение конфиденциальных переговоров, устанавливался на заднем сидении салона автомобиля. Уровень излучения акустического излучателя составлял 75 Дб. В качестве имитирующего переговоры сигнала использовался тест Покровского.

Шумовая «речеподобная» помеха («речевой хор») была предварительно записана на компакт-диск, который проигрывался в процессе проведения измерений в автозвуковой системе. Воспроизводимая шумовая помеха подавалась на виброакустические излучатели через «выходы» автозвуковой системы. Виброакустические излучатели крепились на конструкционные элементы автомобиля в соответствии с расположением контрольных точек. В качестве виброакустического излучателя использовался виброакустический излучатель типа «Копейка».

Структурная схема соединения автозвуковой системы и виброакустического излучателя представлена на рис. 2.

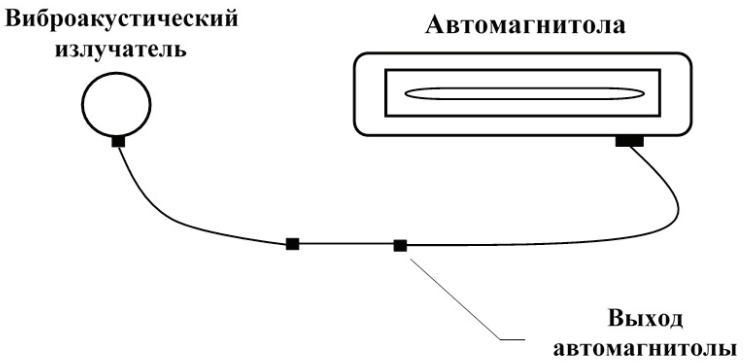


Рис. 2. Структурная схема соединения автомагнитолы и виброакустического излучателя

На приемной стороне в контрольных точках устанавливался виброакустический датчик попеременно в каждой. Виброакустический датчик подключался к многофункциональному поисковому прибору ST031 «Пиранья». Прибор «Пиранья» использовался в режиме виброакустического преобразователя, к нему же подключались наушники. Аудитор в реальном времени записывал отдельные слова услышанного теста. После чего производилась обработка полученных результатов.

Структурная схема экспериментальной установки представлена на рис. 3.

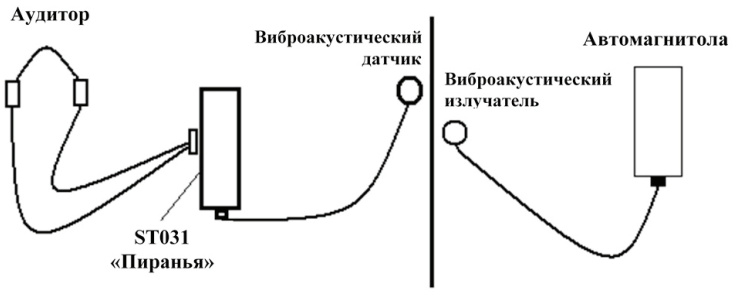


Рис. 3. Структурная схема экспериментальной установки

В процессе проведения анализа защищенности салона была определена зависимость дальности установки виброакустического излучателя от виброакустического датчика на словесную разборчивость переговоров, производимых в автомобиле.

Были выбраны три точки возможной установки виброакустического излучателя «Копейка» при неизменной позиции виброакустического датчика. Позиция 1: расстояние «Копейка» – виброакустический датчик – 10 см; позиция 2: расстояние «Копейка» – виброакустический датчик – 40 см; позиция 3: расстояние «Копейка» – виброакустический датчик – 80 см.

Для проверки степени защищенности речевого сигнала использовался метод речевой разборчивости (по W). При различных условиях – отсутствии и присутствии зашумляющего сигнала – определялось количество правильно перехваченных слов в передаваемом тесте Покровского.

Полученные результаты разборчивости речи, измеренной виброакустическим датчиком с применением Системы защиты № 2, представлены в таблице 3.

Таблица 3

Разборчивость речи при использовании Системы защиты № 2

Номер контрольной точки	Название контрольной точки	Количество правильно принятых слов	Словесная разборчивость в %
Расстояние 10 см			
1	Лобовое стекло	4	8
2	Боковое стекло (переднее)	5	10
3	Заднее стекло	3	6
4	Капот	0	0
5	Боковая дверь (передняя)	0	0
6	Боковая дверь (задняя)	0	0
Расстояние 40 см			
1	Лобовое стекло	10	20
2	Боковое стекло (переднее)	11	22

Окончание табл. 3

Номер контрольной точки	Название контрольной точки	Количество правильно принятых слов	Словесная разборчивость в %
3	Заднее стекло	5	10
4	Капот	2	4
5	Боковая дверь (передняя)	4	8
6	Боковая дверь (задняя)	3	6
Расстояние 80 см			
1	Лобовое стекло	17	34
2	Боковое стекло (переднее)		
3	Заднее стекло	14	28
4	Капот	8	16
5	Боковая дверь (передняя)	10	20
6	Боковая дверь (задняя)	6	12

Выводы

В случае использования предлагаемого метода защиты, как показали данные табл. 2 и 3, для эффективного маскирования информативного сигнала на боковые стекла, задние и передние двери необходима установка по одному виброакустическому излучателю; на лобовое и заднее стекло, капот – по два. Подобная установка виброакустических излучателей со встроенным генератором помех понижает речевую разборчивость до менее чем 10%, при которых практически невозможно установить даже предмет ведущегося разговора.

По результатам измерений был сделан вывод о перспективности использования предложенного метода защиты конфиденциальных переговоров в салоне автомобиля. Наряду с высокой эффективностью он также обладает низкой стоимостью, простотой и комфортом использования, отсутствием необходимости прибегать к использованию дополнительных средств обеспечения комфортабельности проведения переговоров, которые применяются

в большинстве известных средств защиты речевой информации в салоне автомобиля. При использовании рассматриваемого метода перед проведением переговоров не требуется проведение предварительной настройки применяемого оборудования. Кроме того, предложенная система не нуждается в дополнительных источниках питания, так как подключается к собственной автомобильной системе питания.

Примечания

[1] Патент на полезную модель № 143149 от 10.02.2014 «Устройство защиты конфиденциальной акустической информации в салоне автомобиля».

[2] Патент на полезную модель № 87310 от 04.06.2009 «Устройство защиты конфиденциальных переговоров в салоне автомобиля».

[3] *Халяпин Д.Б.* Вас подслушивают? Защищайтесь! М.: НОУ ШО «Баярд», 2004. С. 93.

Е.А. Халепа

ОПЫТ ДОКУМЕНТИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В МОСКОВСКОМ ПРЕДПРИНИМАТЕЛЬСТВЕ В XIX – НАЧАЛЕ XX в.

В статье рассматриваются вопросы использования изобретений в деятельности акционерных компаний в России в XIX – начале XX в. Уделяется внимание роли привилегии как охранного документа на изобретение. Анализируется порядок оформления документов на получение привилегии, регистрацию товарных знаков, фабричных рисунков и изделий.

Ключевые слова: акционерная компания, московское предпринимательство, защита интеллектуальной собственности, документирование, оформление привилегии на изобретение, регистрация товарных знаков и фабричных рисунков.

В XIX – начале XX в. интеллектуальная собственность защищалась привилегиями на изобретения и усовершенствования, регистрацией товарных знаков, моделей, рисунков, образцов продукции.

В соответствии с Положением о компаниях на акциях 1836 г., если акционерная компания создавалась с целью «приведения в действие нового изобретения, сделанного в России или переводимого к нам из чужих краев», то прошению об открытии компании предшествовало прошение о выдаче привилегии на изобретение. Лицо, получившее привилегию на новое изобретение, при необходимости внедрения его в деятельности какой-либо существующей акционерной компании или при создании для этих целей новой компании должно было ей переуступить свою привилегию, оставаясь при этом учредителем компании или просто ее акционером. Акционерным компаниям, созданным в целях реализации изобре-

тений или которым были переуступлены права на изобретения, привилегии предоставлялись на срок действия самой привилегии на изобретение. После этого срока акционерная компания могла продолжать свою деятельность, но уже без привилегии. В соответствии с п. 9 Положения «дарованная компании исключительная привилегия, по истечении срока оной, ни возобновляема, ни продолжаема быть не может»[1].

Привилегия являлась охранным документом на изобретение. Выдача привилегий способствовала развитию торговли, мануфактурного производства, промышленности. Создание крупных мануфактур требовало значительных капиталовложений. Например, в 1698 г. В. Щеголин и другие купцы вложили большие капиталы в создание в Москве Большого суконного двора. Правительство поощряло создание таких компаний предоставлением различных льгот: монопольной продажи изделий, долгосрочных беспошлинных ссуд, права на беспошлинную торговлю, исключительного права на выпуск изделий и др. В 1751 г. в Москве привилегия была выдана указом Сената от 20 сентября купцу Кункину «о делании принадлежащих к священнодействию и церковному благолепию вещей...». Привилегии были предоставлены основателям шелкового производства в Москве. Владелец шелкоткацкой мануфактуры в Москве И. Шелагин в 1798 г. сообщал в Мануфактур-коллегию о том, что «он пока первый и единственный в России использует два механических ленточных стана, которых более ни у кого и ныне нет...» и фабрика доведена «собственным его старанием до такого совершенства...». Москва с XVIII в. становится основным центром шелкоткачества, хлопчатобумажного и суконного производства России. В 30-х годах XIX в. привилегии выдавались на новые образцы прядильных машин, ткацких станков, шелкомотальных машин, «самотканые дороги» и др.[2]

В 60-х годах XIX в. в связи с развитием предпринимательской деятельности и промышленности возникает необходимость в новом патентном законодательстве. В 1866 г. создается Русское техническое общество, в 1867 – Общество для содействия русской промышленности. 20 мая 1896 г. принято постановление Государственного совета об утверждении Положения о привилегиях на изобретения и усовершенствования.

Функции патентного ведомства были возложены на Комитет по техническим делам, созданный при Департаменте торговли и мануфактур. Председателем Комитета являлся директор Департамента. В работе Комитета принимали участие внештатные эксперты, которые предварительно рассматривали заявки на изобретения

и усовершенствования. Комитет состоял из отделов, в которых рассматривались заявки на изобретения и заключения экспертов. На общем заседании Комитета рассматривались спорные вопросы и жалобы по заявкам и привилегиям.

Положение о привилегиях на изобретения и усовершенствования впервые в России вводило вместо единовременных ежегодные пошлины, которые вносились до начала каждого года действия привилегии. Министру финансов предоставлялось право освобождать от уплаты пошлин за первые три года[3].

Привилегиями ограждались исключительные «права пользования изобретениями и совершенствованиями, сделанными в области промышленности» (ст. 1). Привилегии выдавались русским, иностранным подданным, изобретателям и их правопреемникам (ст. 2). Изобретение должно было иметь существенную новизну в полном объеме, в одной или нескольких частях или в сочетании таких частей, хотя бы и известных ранее (ст. 3). Привилегии не выдавались на химические, пищевые, вкусовые вещества и лекарства (ст. 4).

Порядок документирования процесса подачи заявки и выдачи привилегии излагался в ст. 5, 11–14, 18–19 Положения. Прошение подавалось в Комитет по техническим делам. К прошению прилагались полное описание изобретения на русском языке и квитанция об уплате пошлины в размере 30 руб. Документы разрешалось подавать через поверенных. Заявка рассматривалась одним из отделов Комитета по техническим делам с учетом предварительного рассмотрения экспертами. На заседание мог быть приглашен заявитель или его поверенный. Обсуждение и принятие решения осуществлялись при отсутствии заинтересованных лиц. По итогам обсуждения принималось решение о выдаче привилегии в соответствии с прошением, привилегии с изменениями и ограничениями или об отказе в ее выдаче с указанием причин. Заявитель мог обжаловать решение Комитета в течение трех месяцев после получения ответа. При этом требовалось оплатить пошлину в размере 15 руб. в счет рассмотрения дела новыми экспертами.

Требования к изобретению излагались в ст. 6. Его наименование должно было соответствовать действительному значению изобретения. Описание должно было позволять свободно исполнить изобретение и иметь при необходимости чертежи и модели. В конце описания указывались отличительные особенности изобретения. Автор заявки мог в течение трех месяцев от даты подачи заявки корректировать описание без изменений его по существу. Положение 1896 г. впервые определило критерии охраноспособ-

ности изобретения: «существенная новизна» и «промышленная применимость»[4].

Положение 1896 г. вводило выдачу Департаментом торговли и мануфактур «охранительных свидетельств» с публикацией информации в «Правительственном вестнике» и «Вестнике финансов, промышленности и торговли», которые действовали с момента публикации до дня выдачи привилегии. При отказе в выдаче привилегии действие «охранительного свидетельства» прекращалось (ст. 7–9).

Срок действия привилегии в России составлял 15 лет с даты ее подписания. Действие привилегии на изобретение, уже охраняемое за рубежом до даты подачи заявки в России, не могло превышать срока действия привилегии за рубежом (ст. 16). Автор изобретения после принятия решения о выдаче привилегии должен был в течение трех месяцев представить квитанцию об уплате пошлины за первый год ее действия (ст. 16).

Патентная грамота на изобретение включала следующую информацию: имя просителя, даты подачи прошения и подписания патента; описание изобретения; объяснение его особенностей, составляющих новизну; срок действия привилегии; указание, что ранее такие привилегии не выдавались; указание, что правительство не отвечает за принадлежность изобретения заявителю и за пользу изобретения; необходимость использовать изобретение в России не позднее пяти лет с даты подписания патента. Привилегия подписывалась министром финансов и директором Департамента торговли и мануфактур. Объявления о выданных в России привилегиях публиковались в «Правительственном вестнике» и «Вестнике финансов» (ст. 20–21, 24). Подробные описания изобретений и чертежи публиковались в отдельных брошюрах или в ежемесячных сборниках привилегий. Практическое использование изобретения в России не позднее пяти лет со дня подписания привилегии подтверждалось документально фабричным инспектором[5].

Привилегия прекращала действие в следующих случаях: истечение срока действия; неуплата ежегодных пошлин; неиспользование изобретений; решение суда об аннулировании оспоренной привилегии; недостаточность сведений в описании изобретения для его использования без помощи автора. О прекращении срока действия привилегии указывалось в официальных публикациях.

Оформление документов, связанных с защитой изобретений (особенно если предполагалось оформление защиты не только в России, но и в зарубежных странах), требовало значительных затрат времени и труда. Особо тщательно исследование новизны

изобретений проводилось в России и Германии, где рассмотрение новизны осуществлялось Патентными ведомствами и получить привилегию, «широко ограждающую интересы изобретателя», было сложно. Во Франции, Бельгии и ряде других стран порядок выдачи привилегий был «явочным» и отказ мог быть исключительно по формальным причинам[6]. В целях получения привилегии требовалось описать изобретение с такой полнотой, которая была бы достаточна для его воспроизведения, и позволяла четко определить, что в нем является новым и характерным.

Как правило, подготовка документов поручалась «патентным поверенным», которые за определенную плату квалифицированно осуществляли функции, связанные с оформлением материалов по защите интеллектуальной собственности.

В материалах архивного фонда Акционерного общества жирардовских мануфактур «Гилле и Дитрих» в Москве (1883–1917) содержится описание порядка оформления документов при подаче заявок на защиту интеллектуальной собственности. Акционерное общество осуществляло деятельность в сфере галантерейной и швейной промышленности. Акционерным обществом осуществлялась продажа различных тканей: батиста, гипюра, шифона, ситца, сатина, ангоры, вельвета, кашемира и др. В документах архивного фонда содержатся образцы тканей, рисунков, прейскуранты цен на изделия текстильной промышленности, а также описания технологии пошива одежды. Представительства акционерного общества имелись не только в Москве, но и в других городах России, в частности в Серпухове, Астрахани[7].

В документах архивного фонда данного акционерного общества излагается порядок проведения «технических и юридических консультаций» инженером-технологом из Санкт-Петербурга М.С. Снисаренко по вопросам защиты «промышленного творчества» и интеллектуальной собственности[8].

Порядок предоставления услуг в области защиты интеллектуальной собственности излагается М.С. Снисаренко в специальном методическом пособии «Исходатайствование привилегий на изобретения. Регистрация товарных знаков, фабричных рисунков и моделей. Технические и юридические консультации по вопросам защиты промышленного творчества».

В целях оформления привилегии на изобретение предприятие-заявитель выдавало патентному поверенному доверенность установленной формы на каждое изобретение и для каждой страны отдельно, а также описание изобретения с указанием, что в нем является наиболее существенным, и чертежи изделия. В России

доверенность заверялась нотариусом, в Германии, Англии и Франции было достаточно подписи изобретателя без дополнительного «засвидетельствования». В Комитет по техническим делам в России или в соответствующее Патентное ведомство за границей чертежи представлялись в двух экземплярах. Дополнительный третий экземпляр хранился в специальном деле у патентного поверенного. Изготовление чертежей поручалось «технически образованным чертежникам». При пересылке чертежей не допускалось их складывание, требовалась их упаковка между двумя досками или «свертывание в широкую (во избежание поломок и изгибов) трубку из толстой папки».

В стоимость за «исходатайствование привилегии» включались: плата за исправление или дополнение кратких описаний изобретения; пошлинные деньги; гербовый сбор; гонорар и другие мелкие расходы. Особая плата с учетом затраченного времени и труда предусматривалась за составление и изменение чертежей, корректировку или составление новых описаний изобретений, подачу возражений и апелляций в Патентные ведомства зарубежных стран. Тариф на заявление привилегий на изобретения составлял (при сроке действия привилегии в течение 15 лет): в России – 80 руб.; Германии – 60 руб.; Франции – 90 руб.; Японии – 200 руб.[9]

Особенно тщательно охранялись изобретения в военной сфере. В соответствии с «Уложением о наказаниях» «за продажу или предложение за границу привилегий на изобретения, признанные военной тайной, а также за публикацию или сообщение (без разрешения) постороннему лицу секретных сведений полагалось до 8 лет каторжных работ»[10].

С изобретателей брали расписки, ограничивающие их права, связанные с передачей изобретения. В расписках указывалось, что изобретатель не имеет права сообщать об изобретениях никому в России или за рубежом и несет законную ответственность перед правительством. С изобретателем заключалось секретное соглашение об использовании изобретения.

С конца XIX в. широко практиковалось размещение секретных заказов на нескольких частных предприятиях, которые не имели представления о назначении изготавливаемых деталей. В должностных инструкциях работников содержались пункты о сохранении тайны: «...какое тайное дело или какое б оное ни было, которое приказано мне будет тайно содержать, и то содержать в совершенной тайне и никому не объявлять, кому о том ведать не надлежит и не будет повелено объявлять»[11].

При проведении выставок, в том числе и за рубежом (например, Россия принимала участие во Всемирной выставке в Париже в 1900 г.), принимались меры, «чтобы... военно-технические секреты были охранены»[12]. Меры по сохранению тайны изобретений предпринимались не только в военной сфере, но и в промышленности, не связанной с данной областью. Засекречивание являлось также формой защиты прав изобретателя при отсутствии привилегии на изобретение[13].

В XIX – начале XX в. широкое распространение в России получают товарные знаки. Предшественниками товарных знаков являлись графические знаки, устанавливающие авторство производителя, известные с VIII в. до н. э. у китайских оружейников. В XII–XVII вв. получают распространение эмблемы и клейма на продукции изготовителей тканей, фарфора, других товаров. В XVIII в. в Англии товарные знаки появляются на упаковке лекарственных товаров. В XIX в. товарные знаки стали включать рекламную информацию: логотипы, эмблемы, рекламные тексты и др.[14]

В России большая часть товарных знаков включала следующие сведения о предприятии: имя, отчество (допускалось указывать только инициалы) и фамилия владельца или полное наименование; местонахождение. Товарные знаки (торговые марки, этикетки, клейма и другие обозначения, проставляемые на упаковке товаров, изделиях, посуде и др.) регистрировались в Отделе промышленности. Все надписи на товарных знаках составлялись только на русском языке (иностранный язык допускался лишь в виде дополнения). Разрешалось включать в товарные знаки изображения медалей, если они были получены на выставках в России или за рубежом. В последнем случае только при условии, что Россия принимала официальное участие в таких выставках. «Медали должны быть изображены таким образом, чтобы на них отчетливо было видно место выставки и год получения». Каждая медаль изображалась «с лицевой и оборотной стороны таким образом, чтобы одна сторона заходила на половину за другую»[15].

В методическом пособии М.С. Снисаренко, которое названо выше, рассматривался порядок оказания им услуг в сфере регистрации товарных знаков. М.С. Снисаренко получал от предприятия-заявителя доверенность на оказание услуг, 25 экз. товарного знака, нотариально заверенную копию промыслового свидетельства или другого документа, удостоверяющего права предприятия. За содействие в регистрации товарных знаков им взималась плата в размере 25 руб. за один товарный знак, при одновременном оформлении нескольких товарных знаков сумма уменьшалась до

18 руб. за каждый знак. При отказе в регистрации товарного знака и необходимости внесения изменений им однократно оказывалась помощь в новой подаче документов за дополнительную оплату в размере 5 руб. Такой же суммой оплачивалась предварительная экспертиза товарного знака (проверялось, «имеются ли препятствия к утверждению товарного знака»). Если товарный знак принимался к заявке, за него уплачивалась пошлина (12 руб. за 10 лет).

Регистрация фабричных рисунков, моделей, изделий промышленности, технических конструкций и др. осуществлялась «явочным порядком без рассмотрения новизны»[16]. Для подачи заявки сроком на 10 лет М.С. Снисаренко получал от предприятия в трех экземплярах рисунок, модель, образец, а также доверенность установленной формы. Оплата за оформление регистрации рисунков и моделей соответствовала оплате товарных знаков.

Ведение делопроизводства, связанного с оформлением документов по защите интеллектуальной собственности, осуществлялось только после полной оплаты всех работ. В случае отказа в положительном решении вопроса деньги подлежали возврату. При заказах на сумму, превышающую 600 руб., по специальному соглашению допускалась поэтапная оплата[17].

Подводя итоги проведенного исследования, можно сделать вывод о том, что в XIX – начале XX в. порядок документирования деятельности, связанной с защитой интеллектуальной собственности, достаточно четко регулировался законодательно. Однако в связи с высокой трудоемкостью данного процесса и в целях оказания помощи предприятиям, среди которых значительное место занимали акционерные компании, практиковалось издание методических пособий с подробным разъяснением требований к составу и порядку оформления документов, необходимых для получения привилегий на изобретения, а также для регистрации товарных знаков, рисунков и образцов продукции.

Примечания

1 ПСЗ РИ. Собр. 2-е. Т. XI. Отд. 2-е. 1836 год. От № 9494–9824. СПб.: В тип. II Отделения Собственной Е.И.В. Канцелярии, 1837. Ст. 9763.

2 *Афанасьева В.И.* Привилегия как исключительное право в процессе становления и развития мануфактурного производства России // Государство и право. 2005. № 8. С. 69–76.

3 *Афанасьева В.И.* Патентное право в России (на примере Положения о привилегиях на изобретения и усовершенствования 1896 г.) // Там же. 2007. № 2. С. 113.

[4] Там же. С. 116.
[5] Там же. С. 114–116.
[6] ГБУ «ЦГА Москвы». Центр хранения документов до 1917 года. Ф. 316. Оп. 1. Д. 669. Л. 3.
[7] Там же. Л. 13–13 об.
[8] Там же. Л. 3–7 об.
[9] Там же. Л. 3 об.–5 об.
[10] *Юркин И.Н., Пинк И.Б.* «Проникнуть в самый секрет изобретения...» // Вопросы истории естествознания и техники. 2007. № 2. С. 69.
[11] Там же. С. 67–68.
[12] Там же. С. 70.
[13] Там же.
[14] *Романова Т.П.* Из истории торговых марок в России // Этнографическое обозрение. 2007. № 1. С. 132–134.
[15] ГБУ «ЦГА Москвы». Центр хранения документов до 1917 года. Ф. 316. Оп. 1. Д. 669. Л. 6–6 об.
[16] Там же. Л. 6 об.–7.
[17] Там же. Л. 7 об.

Е.В. Сидоренко

РОЛЬ ДОКУМЕНТОВ В СИСТЕМЕ МЕНЕДЖМЕНТА КАЧЕСТВА

В предлагаемой статье освещаются некоторые ключевые моменты системы менеджмента качества, касающиеся работы с документами. Особое внимание уделяется значению документации в управлении качеством, предпринимается попытка определить новую роль документов в управлении через анализ требований к построению и структуре пакета документов как в государственной, так и в коммерческой организации. Рассмотрены факторы, влияющие на эффективность документов как инструмента управления качеством.

Ключевые слова: документ, система менеджмента качества, регламентация, качество, документированные процедуры.

Сегодня мы, говоря о деятельности коммерческой организации или предприятия любой организационно-правовой формы, сталкиваемся с новыми требованиями к управлению. В условиях ужесточившейся конкуренции меняются задачи, стоящие перед руководством: эффективность деятельности организации должна стать выше, в то же время количество затрачиваемых финансовых, материальных и прочих видов ресурсов должно быть сокращено. Для руководства организации актуальным вопросом становится поиск все более эффективных принципов управления, способных удовлетворить требованиям современности.

Наука управления также не стоит на месте, предлагая различные подходы к управлению. Одним из самых востребованных сегодня подходов к управлению является Система менеджмента качества (СМК), предлагающая по-новому взглянуть на отдельные аспекты управления, влияющие на качество и эффективность дея-

тельности организации[1]. Тема внедрения системы менеджмента качества в управление организацией, ее преимущества и недостатки изучена уже достаточно подробно, но одному из аспектов, на наш взгляд, уделено недостаточно внимания – это роль документов в управлении качеством. СМК открывает огромные перспективы в области управления документами как эффективного инструментария управления организацией. Изучение данного вопроса позволит нам определить новую роль документа в управлении.

С 70-х годов прошлого века началась активная деятельность по разработке стандартов ИСО по системе менеджмента качества с рекомендациями, позволяющими построить СМК с нуля в любой организации. Сегодня стандарты ИСО признаны во всем мире. Документам стандарты ИСО отводят одну из главных ролей в вопросах управления качеством. Разделы о документировании деятельности, составе пакета регламентирующих документов, структуре и требованиях к информации есть во всех стандартах[2]. В каждом из них подчеркивается, что документ отражает принятые решения, фиксирует результаты деятельности, позволяя их сопоставить с запланированными, описывает последовательность действий. Значение документа, таким образом, становится очень многогранным, а качество содержащейся в нем информации приобретает первостепенное значение как характеристика деятельности всей организации.

Основной идеей стандартов ИСО является идея разделения процесса производства или оказания услуги на ряд типовых повторяющихся операций. Качественное выполнение каждой из этих операций влияет на качество конечного продукта. Чтобы этого добиться, порядок выполнения каждой операции должен быть регламентирован и задокументирован, а формы документов, образующихся в процессе выполнения работ, унифицированы. Поэтому под документами в стандартах подразумеваются именно регламентирующие документы: руководства, инструкции, а также унифицированные формы. То есть речь идет о документах, которыми сотрудники руководствуются при выполнении своих ежедневных должностных обязанностей. Регламентирующие документы, таким образом, являются значимым, но недооцененным инструментом управления качеством.

Обратимся напрямую к стандартам.

ИСО 9000 так определяет значение документации (п. 2.7.1)[3]:

«Документация дает возможность передать смысл и последовательность действий. Ее применение способствует:

а) достижению соответствия требованиям потребителя и улучшению качества;

б) обеспечению соответствующей подготовки кадров;
в) повторяемости и прослеживаемости;
г) обеспечению объективных свидетельств;
д) оцениванию эффективности и постоянной пригодности системы менеджмента качества».

Более подробно о роли документов в организации рабочих процессов организации находим в ИСО 15489 (разд. 4):

«Документы содержат информацию, являющуюся ценным ресурсом и важным элементом деловой деятельности. Системный подход к управлению документами позволяет организациям и обществу защищать и сохранять документы в качестве доказательства действий. Система управления документами позволяет создать информационный ресурс о деловой деятельности, который может поддерживать последующую деятельность и отдельные решения, а также обеспечивать подотчетность всем заинтересованным сторонам.

Документы позволяют организациям:
– осуществлять свою деятельность упорядоченно, эффективно и подотчетно;
– предоставлять услуги последовательно и беспристрастно;
– обеспечивать и документировать формирование политики и принятие управленческих решений;
– обеспечивать согласованность, непрерывность и производительность деловой и управленческой деятельности;
– повышать эффективность деятельности всей организации;
– обеспечивать бесперебойность деятельности в случаях чрезвычайных ситуаций;
– соблюдать требования законодательства и регулирующей среды;
– обеспечивать защиту и поддержку в судебных делах;
– защищать интересы организации и права сотрудников;
– обеспечивать и документировать текущие и будущие научно-исследовательские и опытно-конструкторские работы, деятельность по развитию, разработки и достижения;
– предоставлять документированные доказательства деловой, личной и общественной деятельности;
– обеспечивать деловое, персональное и социальное своеобразие;
– сохранять корпоративную, индивидуальную память, память общества».

Таким образом, вырисовывается несколько важнейших функций документа:

1. С точки зрения управления:

1.1. Документ обеспечивает принятие управленческих решений. Управление основывается на получении и передаче информации от управляемых объектов к лицу, принимающему управленческое решение, и наоборот. Именно на основе полученной информации и принимается управленческое решение, которое должно быть доведено до исполнителя. Это предъявляет определенные требования к движению информации именно ввиду ее роли в управлении. Поскольку информация сама по себе нематериальна, то огромную роль играет документ, фиксирующий ее и придающий ей материальность. Таким образом, документ становится инструментом управления, так как позволяет передавать информацию для принятия управленческого решения. В этом заключается зависимость качества управления от документооборота.

1.2. Документирование позволяет планировать и контролировать деятельность путем фиксирования требуемых показателей с последующим сопоставлением их с достигнутыми результатами. По результатам сравнения принимается управленческое решение о применении корректирующих действий, если это необходимо.

1.3. Наличие документированных процедур с четко прописанными критериями принятия решения придает прозрачность управлению. Управленческое решение принимается исходя из анализа имеющейся информации на предмет ее соответствия критериям, заданным в регламентирующем документе. Этот фактор особенно важен для тех организаций, деятельность которых контролируется обществом, – это прежде всего органы государственной власти и муниципальные учреждения, а также общественные организации и организации, созданные в форме открытых акционерных обществ.

2. С точки зрения производственного процесса:

2.1. Документ фиксирует смысл и передает последовательность действий при выполнении типовых повторяющихся процедур. Здесь речь идет о рабочих инструкциях, описаниях процесса и процедур, содержащих пошаговое описание выполнения работ, сроки, ссылки на взаимосвязанные процессы. Соблюдение работником инструкции обеспечивает необходимый уровень качества и сокращает сроки на выполнение операции.

2.2. При создании регламентирующих документов описываемый объект, будь то структура организации или рабочая операция, подлежит анализу и оптимизации. Признаком профессионального подхода к процессу регламентации является постоянный поиск возможностей для повышения эффективности деятельности орга-

низации, идет ли речь о схеме движения документов или распределении обязанностей между отделами.

2.3. Применение унифицированных форм документов, образующихся в процессе выполнения рабочих операций, позволяет контролировать документообразование, препятствует неконтролируемому росту документооборота, делает возможными дальнейшую автоматизацию рабочих процессов и сокращение времени на обработку информации.

Для выполнения документами своих функций в организации они должны представлять собой единый массив, систему, на создание и поддержание которой выделяются человеческие и материальные ресурсы. Наличие инструкции по выполнению одной операции вряд ли позволит заметно повысить качество всего процесса. Разработка и внедрение пакета документов, регламентирующих структуру, рабочие процессы, должностные обязанности сотрудников, напротив, делает возможным повышение качества работы всей организации. Поэтому стандарты ИСО предписывают формирование пакета регламентирующих документов. Документы должны быть построены в строгом иерархическом порядке и иметь каждый свою область применения, свое назначение и функцию, но в то же время быть связаны друг с другом через ссылки и примечания с указанием источников дополнительной информации. Именно системой регламентирующих документов обеспечивается жизнедеятельность системы менеджмента качества, а за ней качество и эффективность деятельности всей организации.

Минимально необходимый состав пакета регламентирующих документов закреплен в ИСО 9001 и предполагает наличие следующих документов[4]:

а) документально оформленные заявления о политике и целях в области качества;
б) руководство по качеству;
в) документированные процедуры и записи;
г) документы, включая записи, определенные организацией как необходимые ей для обеспечения эффективного планирования, осуществления процессов и управления ими.

Состав документов остается на усмотрение самой организации, он может быть расширен (могут быть созданы такие документы, как планы качества, технические требования, методические документы и др.), но не сокращен (в том случае, если организация претендует на получение сертификата о внедрении системы менеджмента качества). Названия документов также носят рекомендательный характер, оставаясь на усмотрение организации.

В российской практике документационного обеспечения управления некоторые виды документов, перечисленные в стандартах как рекомендуемые, не используются. Например, инструкция как документ существует во многих российских организациях только в виде должностной инструкции и инструкции по делопроизводству. В большинстве же западноевропейских компаний инструкция по выполнению работ является одним из самых востребованных документов и представляет собой официальный документ, оформленный должным образом, с предписанными реквизитами, утвержденный вышестоящим руководством. Инструкция с пошаговым описанием выполнения рабочей операции используется всеми сотрудниками, к чьим обязанностям относится выполнение работ на регламентированном участке, ее применение позволяет контролировать качество выполнения работ, обеспечивая соответствие заданных показателей деятельности достигнутым.

Так же обстоит ситуация и с унифицированными формами. Значение унифицированных форм документов для качества управленческой деятельности было отмечено еще в 80-х годах XX в., когда были разработаны одни из первых стандартов в данной области[5]. ГСДОУ, утвержденная в 1988 г.[6], также определяла роль унифицированных форм документов для «совершенствования работы аппарата управления»[7] и обеспечения «единства правил документирования управленческих действий на всех уровнях управления»[8].

Государственные стандарты и система документационного обеспечения управления регулировали прежде всего работу с управленческой и кадровой документацией, что нашло продолжение в современных российских стандартах. Но ведь есть еще достаточно большой массив документации, создаваемый в рамках рабочего процесса. Его образование не подлежит учету и контролю, в то же время такая документация содержит в себе большой объем информации о деятельности организации, что, как мы уже выяснили, является ценностью. В процессе выполнения типовых повторяющихся операций образуются одни и те же виды документов, и разработка унифицированных форм для них представляется эффективным механизмом повышения скорости обработки информации, улучшения качества работы, а также контроля за документообразованием.

Таким образом, стандарты ИСО открывают новые возможности использования документа для повышения качества деятельности организации. Выделяется отдельная категория документации по управлению качеством, требования к которой сформулированы в международных стандартах системы менеджмента качества.

В российских традициях документирования деятельности организации документы, не относящиеся к управленческой, кадровой или финансовой системам документации, остаются вне сферы регулирования, их создание и жизненный цикл не регламентированы. В то же время из практического опыта международных организаций, в том числе работающих в России, мы видим, что в деятельности любой организации существует определенный пакет документов, используемых в повседневной работе. Эти документы не только описывают «что делать», но и «как», и «когда», они закрепляют общую цель и направление развития организации, определяют роль каждого сотрудника в достижении этой цели, что является прекрасной мотивацией качественнее выполнять должностные обязанности. Стандарты по системе менеджмента качества относят документацию такого рода к документации по управлению качеством, определяют ее роль во внутренних процессах организации, выделяют как постоянную функцию управления этими документами. Таким образом, международный опыт в вопросах организации деловой деятельности предлагает нам по-новому взглянуть на документы, регламентирующие порядок выполнения типовых повторяющихся операций, и расширить их использование в организациях любой организационно-правовой формы и любой сферы деятельности. Основная идея системы менеджмента качества в области документирования состоит в том, что документ становится современным инструментом управления качеством. Поэтому большое внимание уделяется поддержанию пакета регламентирующих документов в рабочем состоянии, что является постоянной функцией организации и характеристикой СМК, определяющей качество управления организацией и конечной продукции или услуги.

Успешность и эффективность публичных компаний, внедривших систему менеджмента качества, привели к тому, что принципы управления качеством стали применяться и в государственном управлении в США, странах Западной Европы и России, что стало результатом проводимых правительством этих стран административных реформ. Основными задачами реформирования были сокращение государственных расходов, повышение эффективности государственного управления и привлекательности государственной службы, совершенствование оказания государственных услуг[9]. К решению данных задач и были привлечены новейшие технологии управления, доказавшие свою универсальность на примере публичных компаний. Чем же объясняется эффективность основных принципов управления качеством в столь разных организациях?

Управление призвано решать стоящие перед ним цели и задачи наиболее эффективно. С развитием общества и информационных технологий набор задач постоянно меняется, требуя выработки новых подходов и методов управления. Это четко можно проследить в государственном управлении. Смена политической системы ставит новые задачи, для решения которых требуются более совершенные инструменты.

После распада СССР и образования Российской Федерации стала очевидной неэффективность существовавших на тот момент органов исполнительной власти. Поэтому основной целью административной реформы, первый этап которой был начат в 1991 г., было повышение эффективности деятельности государственного аппарата, придание открытости и прозрачности процессам управления, широкое использование информационных технологий.

Инструментом оптимизации исполнения государственных функций и оказания государственных услуг стал административный регламент оказания государственных услуг и исполнения государственных функций[10]. Административный регламент прописывает порядок работы и движение документов в процессе предоставления государственной услуги. Он является инструментом управления качеством оказания государственных услуг, определяя требования и позволяя соотнести степень соответствия характеристик зафиксированным требованиям. В то же время административный регламент является инструкцией для исполнителя, описывая последовательность действий и критерии принятия решения.

Его внедрение в деятельность органов исполнительной власти на первом этапе реформы должно было способствовать сокращению объема документооборота, срока оказания услуги или выполнения государственной функции, упорядочению административных процедур. Несомненно, эти задачи сложны и многоаспектны. Для их решения был использован один из методов СМК – регламентация и документирование типовых повторяющихся процедур.

По составу информации административный регламент по оказанию государственных услуг, разрабатываемый с учетом требований международных стандартов в области управления качества, близок к руководству по качеству и описанию процесса, так как содержит стандарт качества и описывает последовательность действий, при выполнении которых услуга будет оказана качественно. Именно четкое прописывание порядка работы с документами и критериев принятия решений позволяет решить задачи, стоящие перед государственным аппаратом.

Таким образом, механизмы, применяемые для повышения качества как в государственном, так и в корпоративном управлении, основаны на подробной регламентации типовых повторяющихся операций. Основным инструментом управления качеством выступает документ, точнее система документации, разработанная с учетом международных стандартов по управлению качеством.

Примечания

1 *Василенко И.* Возможности и границы использования инновационных бизнес-технологий в административной реформе // Гос. служба. 2010. № 2. С. 28–31; *Исаев С.В.* Документация в системах менеджмента // Методы менеджмента качества. 2007. № 5. С. 41–44; *Ларин М.В.* Управление документами на основе международного стандарта ИСО 15489-2001. М.: ВНИИДАД, 2005. 110 с.; *Митченко О.Ю.* Требования к системе управления документами (по международному стандарту ИСО 15489-2001) // Секретарское дело. 2005. № 4. С. 58–62; *Пономарева Т.А.* Процессный подход к оценке внутреннего качества в сервисной организации // Менеджмент в России и за рубежом. 2005. № 4. С. 74–81; *Сокова А.Н.* Делопроизводство предприятия в системе управления качеством на основании стандартов ИСО серии 9000 и стандартов России // Делопроизводство. 2001. № 2. С. 34–39; *Суровцева Н.Г.* Документация системы менеджмента качества. Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2010. 169 с. и др.

2 ISO 9000:2001. Quality management systems. Fundamentals and vocabulary; ISO 9001:2008. Quality management systems – Requirements; ISO 15489-1. Information and documentation – Records management; etc.

3 ISO 9000-2001. Quality management systems. Fundamentals and vocabulary.

4 ГОСТ Р ИСО 9001-2008. Системы менеджмента качества. Требования. М.: Стандартинформ, 2009.

5 ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения [Электронный ресурс] // Информационно-справочная онлайн система «Технорма.RU». URL: http://www.tehnorma.ru/gosttext/gost/gost_1976.htm (дата обращения: 10.01.2015); ГОСТ 6.10.5-87. Унифицированные системы документации. Требования к построению формуляра-образца [Электронный ресурс] // Там же. URL: http://www.tehnorma.ru/gosttext/gost/gost_2266.htm (дата обращения: 15.01.2015).

6 Государственная система документационного обеспечения управления. Основные положения. Общие требования к документам и службам документационного обеспечения. М.: Главархив СССР, 1991.

[7] Там же. П. 1.2.

[8] Там же. П. 2.1.2.

[9] *Жукова Е.Н.* Исполнительные агентства Великобритании // Журнал российского права. 2009. № 6. С. 132–140; *Капаров С.Г.* Стандарты предоставления государственных услуг – новый этап административной реформы в Казахстане [Электронный ресурс] // ЧиновникЪ. URL: http://chinovnik.uapa.ru/ru/issue/2004/05/14/ (дата обращения: 15.01.2015); *Кузьмин В.В.* Генезис «менеджерской модели» государственной службы (на примере Великобритании) // История государства и права. 2007. № 7. С. 35–37; Процессный подход в стандартах ИСО серии 9000 и на практике / Кол. авт.; под общ. ред. Г.Е. Герасимовой. М.: ООО «НТК Трек», 2006. 168 с.; ил.; Document management in the European Commission. Collected decisions and implementing rules [Электронный ресурс] // European Commission. URL: http://ec.europa.eu/transparency/archival_policy/docs/edomec/recueil_dec_mda_en.pdf (дата обращения: 15.01.2015); и др.

[10] *Федосеева Н.Н.* Административные регламенты как инструмент современного государственного управления // Государственная власть и местное самоуправление. 2009. № 6. С. 7–12; *Хабриева Т.Я., Ноздрачев А.Ф., Тихомиров Ю.А.* Административная реформа: решения и проблемы // Журнал российского права. 2006. № 2. С. 3–23; *Игнатюк Н.А.* Административные регламенты федеральных органов исполнительной власти: вопросы методологии // Там же. № 10. С. 29–34 и др.

В.А. Степанов

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОГО РЕГИСТРА В СТРУКТУРЕ АДМИНИСТРАЦИИ НАЦИОНАЛЬНЫХ АРХИВОВ И ДОКУМЕНТАЦИИ: ИСТОРИЯ СОЗДАНИЯ И ЕГО РОЛЬ В ГОСУДАРСТВЕННО-ПРАВОВОМ РЕГУЛИРОВАНИИ

В статье рассматривается историческое развитие, назначение и роль важнейшего структурного подразделения Администрации национальных архивов и документации США, а именно Управления Федерального регистра; дается детальное описание истории формирования Управления, его правовой статус; показывается степень участия Управления в политических процессах.

Ключевые слова: Федеральный регистр, публикации, документы, законодательство.

Управление Федерального регистра является структурным подразделением архивно-документационной службы США Администрации национальных архивов и документации. В рамках своей деятельности, охватывающей практически 80-летний период, Управлением была выполнена грандиозная работа по выстраиванию информационной системы взаимодействия государственного аппарата и гражданского сектора. Ознакомлению с историей и определению роли данного Управления в системе государственного регулирования и посвящена данная статья.

Образование в середине 1930-х годов в системе Национального архива Отдела Федерального регистра произошло в рамках адаптации государственного аппарата США и расширения его регулятивных функций для решения задач «Нового курса» президента Франклина Д. Рузвельта.

В тот период американская экономика достигла лишь относительных успехов в промышленности, благодаря чему США занимали

первое место в мире по производству в совокупности с другими ведущими государствами[1]. Несмотря на это, Великая депрессия сильно ударила по позициям малоимущих слоев населения, спровоцировав рост безработицы и ослабление финансового потенциала страны. В начале 1930-х годов необходимость реализации экономических программ и политического курса по выходу из Великой депрессии привела к смещению центра тяжести политики в США на исполнительную власть. На институциональном уровне это проявлялось в создании все новых учреждений, ведомств. В то же время расширение регулятивной роли федеральных учреждений исполнительной власти в социальной и производственной сфере с целью предотвращения кризиса привело к разрушительным последствиям для законодательства в целом, внеся хаос в систему нормотворчества[2].

Зачастую большинство инициатив, которые предлагались администрацией президента США Франклина Д. Рузвельта в качестве экстренных мер, отклонялись Верховным судом, так как они не соответствовали конституционным нормам, каковыми, например, являлись положения закона «О восстановлении промышленности» и ряд других актов, связанных с ним[3].

Столкнувшись с жесткими политическими реалиями и стараясь найти способ решения проблемы, Конгресс США фактически наделил федеральные учреждения исполнительной власти широчайшими законодательными полномочиями, что, в свою очередь, привело к появлению ряда бессистемных нормативных документов. Данная ситуация явилась главной причиной, побудившей правительство к проведению реорганизации и упорядочиванию системы нормотворчества.

Становилось очевидным, что огромный поток административных постановлений противоречил самим законам и приводил к серьезным правовым проблемам. Известны случаи, когда государственные адвокаты, обращаясь в Верховный суд с исками по конкретным делам, узнавали, что ряд подзаконных актов просто не соответствовал существующим юридическим нормам[4].

Это побудило к действию многих авторитетных юристов и политиков, оказавших значительное влияние на появление первого официального периодического издания нормативных актов федеральных учреждений исполнительной власти в США. Одним из них был Эрвин Грисволд, главный юридический консультант страны, написавший в 1934 г. критическую статью в «Harvard Law Review», в которой негативно оценивал состояние регулятивной деятельности государственных учреждений. К статье прилагался текст законопроекта, который с точки зрения Э. Грисволда должен

был стать основой для формирования упорядоченной системы нормативных актов[5].

Статья нашла отклик в политических кругах. Эмануэль Селлер, член подкомитета Судебного комитета Палаты представителей с 1934 г., ознакомился с текстом предложенного законопроекта и обсудил его с Э. Грисволдом. Затем, в марте 1935 г., Э. Селлер внес редакцию данного закона на обсуждение в Сенат, который принял закон после короткого обсуждения без каких-либо возражений[6].

По инициативе правительства подписанный президентом США Ф.Д. Рузвельтом 26 июля 1935 г. был утвержден закон «О федеральном регистре», нормы которого по предметам их ведения кодифицированы в положениях № 1501–1511, в 44 титуле (разделе) (Публичные издания и документы) «Свода законов США»[7]. В соответствии с законом создавался Отдел Федерального регистра как структурное подразделение сформированного в 1934 г. независимого федерального архивного учреждения – Национального архива. Главной задачей Отдела Федерального регистра являлась официальная регистрация, хранение и публикация нормативных документов центральных федеральных учреждений исполнительной власти в ежедневном периодическом издании (газете) «Федеральный регистр».

Таким образом, формирование Отдела, в деятельности которого с течением времени стали органично сочетаться функции архивного, юридического и издательского учреждений, было обусловлено потребностями централизованного контроля над масштабной нормотворческой деятельностью государственного аппарата, ставшей следствием активизации государственного вмешательства в экономику страны и решения социальных проблем.

Следует особо отметить, что закон «О федеральном регистре» впервые в истории США установил систему обязательной государственной регистрации и публикации актов нормотворческой деятельности администрации и особо подчеркивал, что факт публикации административного акта в издании «Федеральный регистр» приобретает важные правовые последствия, так как означает «своевременное и действительное оповещение» всех лиц, на которых оно распространяется, о наличии и содержании акта, что исключает ссылку таких лиц на незнание о его существовании.

Для управления Отделом был сформирован руководящий аппарат в лице Административного комитета, в состав которого входили руководитель Национального архива – архивист США, представитель Министерства юстиции, директор Отдела Федерального регистра и глава Государственного издательства. В рамках сотруд-

ничества с Отделом Федерального регистра Государственное издательство занималось непосредственным изданием «Федерального регистра», первый выпуск которого состоялся 14 марта 1936 г.[8]

По положению № 1505 закона «О федеральном регистре», в 44 титуле (разделе) «Свода законов США» к составу публикуемых Отделом материалов Федерального регистра были отнесены[9]:

– Федеральные законы;
– Президентские документы;
– Административные постановления;
– Публичные речи;
– Описания федеральных организаций, их программ и инициатив.

Административный комитет обеспечил прочную связь Отдела Федерального регистра с федеральными учреждениями исполнительной власти и законодательным органом страны – Конгрессом США, благодаря чему Отдел осуществлял широкую деятельность в законодательной сфере.

В период Второй мировой войны Отдел Федерального регистра сыграл значительную роль в укреплении взаимоотношений между Национальным архивом, структурным подразделением которого он являлся, и федеральными учреждениями. Количество изданных документов в каждом отдельном выпуске FR за период с 1941 по 1943 г. составляло от 7 850 до 18 569. Природа информации, содержавшейся в документах, отражала хозяйственное положение страны в период Второй мировой войны: ценовые графики, государственные заказы, положения о контроле за экспортом и услугах, нормированные заказы, документы об иностранцах, потребительский кредит, учреждение новых военных ведомств[10].

Подчеркнем, что сотрудники Отдела проводили консультации с федеральными учреждениями по вопросам издания нормативных актов на момент военного положения, а также кадровой политики и усовершенствования управления путем ускорения процесса принятия решений, которые фиксировались непосредственно в документах[11].

Во время войны начала действовать ежедневная практика телефонирования, связанного с консультациями по вопросам текущего делопроизводства. В частности, это касалось комплексов документов, которые должны были публиковаться в «Федеральном регистре» на следующий день. Некоторые учреждения содержали многочисленные штаты машинисток, чтобы копировать документы прежде, чем они должны были быть напечатаны в очередном выпуске[12]. Военный период показал, что в результате тотальной

загруженности бюрократического аппарата, наличия организационных пробелов и недостаточной степени осведомленности о деятельности различных учреждений возникла необходимость в срочном решении этой проблемы.

В послевоенное время Отдел Федерального регистра встал на путь новых организационных трансформаций, напрямую связанных с принятием 11 июня 1946 г. федерального закона «Об административной процедуре»[13]. Закон усилил связь Отдела с федеральными учреждениями, которые с этого момента были обязаны передавать сведения о законодательных проектах и предоставлять возможность их комментирования общественностью. Данное требование было прописано в положении № 552, пункте А, где отмечалось, что «каждое учреждение в соответствии с законами должно предоставлять свободный доступ к ознакомлению и обсуждению итоговых мнений, интерпретаций политики, административным руководствам и инструкциям, копиям документов и иной справочной информации, которая может потребоваться для поиска необходимых сведений»[14].

Ранее практика комментирования общественностью административных решений в США не предусматривалась[15].

Реорганизация Национального архива в Службу национальных архивов и документации в начале 1950-х годов, вошедшую в состав Администрации общих служб на основании закона от 1949 г. «О федеральной собственности и административных службах»[16], привела к преобразованию Отдела в Управление Федерального регистра.

С усилением роли президентской власти США в управлении все более усложняющимся обществом и постоянным развитием системы публикации нормативных документов федеральных учреждений расширялись и возможности Управления Федерального регистра. Теперь, помимо подготовки публикаций «Федерального регистра» и Свода федеральных нормативных актов, на Управление были возложены функции подготовки к публикации новых типов документальных собраний, правительственных справочников, методических пособий по делопроизводству для учреждений.

К основным серийным публикациям Управления Федерального регистра отнесем издаваемые и по настоящее время «Полное собрание законов Соединенных Штатов»[17]; «Компиляция коллекции президентских документов», «Официальные бумаги президентов»[18]; «Руководство правительства Соединенных Штатов»[19]; «Публичные и частные акты»[20]; «Пособие по составлению документа»; «Частноправовые издания»[21]. Управление Федерального регистра также издает «Информационный бюллетень» (Federal

Register Bulletin), который представлен на официальном портале Администрации национальных архивов и документации[22].

В течение 1970-х годов некоторые публикации претерпели структурные изменения. Не осталось незамеченным и участие Управления Федерального регистра в разработке инновационных проектов в сфере делопроизводства, в частности в вопросе о переоформлении управленческих документов. Сущность идеи заключалась в том, чтобы унифицировать систему документооборота и облегчить процесс принятия управленческих решений, что в конечном итоге было успешно реализовано и взято федеральными учреждениями на вооружение[23].

Детализированные требования Управления по подготовке исполнительными учреждениями передаваемых документов к официальной публикации изложены в разработанном им методическом материале – «Пособии по составлению документа». В какой-то мере оно сопоставимо с российскими «Правилами издания исторических документов». Пособие служит для предварительной подготовки документов. Прежде чем учреждение передает нормативные документы к публикации в «Федеральный регистр» и Свод федеральных нормативных актов, его руководство должно позаботиться об их унифицированном оформлении, соответствующем основным требованиям Пособия. Отличительной чертой Пособия является целевая направленность на публикацию систематизированной документальной информации.

Период с 1980-х годов по настоящее время представляет собой новый этап в истории Управления Федерального регистра, связанный с процессом реорганизации Службы национальных архивов и документации в Администрацию национальных архивов и документации и возвращения последней статуса независимого федерального исполнительного учреждения США. С развитием информационных технологий, ознаменовавшимся появлением Интернета, изменилась и роль Управления Федерального регистра в системе структурных подразделений Администрации национальных архивов и документации. Сетевое пространство открыло перед Управлением новые возможности, которые оказали значительное влияние на качество публикаций.

Общедоступность и прозрачность – два важнейших качества, которые характеризуют развитие информационных технологий на современном этапе. Управление Федерального регистра, обращаясь к собственному историческому опыту, заложило основы для формирования свободного информационного пространства, в течение последних 20 лет занимаясь переводом печатных изданий

«Федерального регистра» и других публикаций в цифровой формат. Интернет предоставил возможности, которые в значительной степени расширили информационный потенциал Федерального регистра, усилив его влияние в общественной и государственной сферах, а также обеспечив доступ к систематизированной нормативной информации федеральных учреждений исполнительной власти в режиме онлайн для ознакомления и использования гражданами США, государственными учреждениями и частными организациями (чаще всего юридическими фирмами).

Этому способствовали не только многолетнее сотрудничество Управления Федерального регистра и Государственного издательства, но и утвержденный Конгрессом США 22 марта 1993 г. акт «Об улучшении доступа к электронной информации». Положение № 4101, 44 титула (раздела) «Свода законов США», гласило, что «необходимо разработать систему обеспечения онлайн-доступа к документам Конгресса, Управления Федерального регистра и другим публикациям, определенным управляющим документами»[24]. Начиная с 1994 г. на официальном сайте Государственного издательства уже начали размещаться выпуски «Федерального регистра» в цифровом формате, а также другие публикации Управления Федерального регистра.

В свою очередь, федеральные учреждения изъявили желание использовать новые возможности информационных технологий путем передачи нормативных документов в электронной форме непосредственно в Управление. Единственным серьезным препятствием на пути оставалось удостоверение подлинности документов через электронную подпись. Совместно с Государственным издательством Управление запустило в 2001 г. «Электронную систему редактирования и публикации», сокращенно «eDOCS». Назначение этой системы заключалось в промежуточной обработке поступающих из федеральных учреждений документов для их дальнейшего опубликования в «Федеральном регистре»[25].

Однако Управление пошло по пути полной интеграции в пространство Интернета. Результатом стал запуск неофициального сайта «Федеральный регистр 2.0» 26 июля 2010 г. Это был результат усилий Управления, направленных на расширение доступа к социальной, экономической, научной и политической информации. Одновременно подчеркнем, что официальным изданием Управления до сих пор считается печатное издание «Федерального регистра» и его цифровой вариант, публикуемый на сайте Государственного издательства[26].

Управление Федерального регистра также принимает активное участие в организации избирательной системы в США, точнее,

в работе Коллегии выборщиков – старейшего института США, в котором работают лица, представляющие свой штат на народном голосовании, где избираются президент США и вице-президент. Положение Коллегии выборщиков в избирательном процессе установлено Конституцией США (ст. II, разд. I), где определено, что президент и вице-президент избираются «выборщиками» от каждого штата в количестве, равном числу сенаторов от этого штата в Конгрессе. Наличие Коллегии выборщиков освобождает Конгресс США от необходимости избирать президента и вице-президента. Следует напомнить, что последним избранным Конгрессом главой США был 6-й президент Дж.К. Адамс (1825–1829).

Взаимодействие Управления с Коллегией выборщиков осуществляется по линии заверения – сертификации избирательных бюллетеней – свидетельств о проведенных в штатах выборах[27]. Выполнение данной функции осуществляется после того, как из федерального правительства поступит указание распространить инструкции губернаторам штатов о проведении выборов[28]. Таким образом, Управление Федерального регистра играет роль координатора указанного процесса.

Известны случаи, когда бюллетени оказывались недействительными, так как были неправильно составлены, поэтому процесс сертификации должен быть тщательно контролируем. Уже после передачи бюллетеней все полученные голоса в строгом порядке передаются в Конгресс на утверждение. В начале января года, следующего за годом выборов, перед очередной сессией Конгресса председатель Сената Конгресса объявляет о признании выборов действительными и новый президент и вице-президент вступают в должность с 20 января.

Помимо участия в избирательном процессе, Управление взаимодействует с Конгрессом США и штатами, публикуя в «Федеральном регистре» информацию о принятых поправках к Конституции по результатам большинства проголосовавших штатов[29]. Когда три четверти штатов (38) ратифицируют поправку, в Управление передаются все их ратификационные документы. Архивист США свидетельствует об этом в особой декларации, которая публикуется Управлением Федерального регистра в очередном издании «Федерального регистра» и в «Полном собрании законов Соединенных Штатов». При этом поправка к Конституции США приобретает юридическую силу непосредственно с момента публикации в «Федеральном регистре».

Управление Федерального регистра как подразделение Администрации национальных архивов и документации США является

уникальным учреждением, не имеющим аналогов в структуре других архивных служб мира. Конечно, опыт деятельности Управления Федерального регистра нельзя рассматривать вне конкретно-исторических условий США и особенностей организации их архивно-документоведческой отрасли. Однако его изучение и адекватная квалификация, безусловно, необходимы в целях выработки приоритетов развития отечественной модели архивной системы в соответствии с потребностями информационного общества.

Примечания

1 История новейшего времени стран Европы и Америки. 1918–1945. М., 1989. С. 172–173.

2 Another Regulatory Milestone: The Federal Register Act Turns 75 [Электронный ресурс] // Regblog. URL: http://www.regblog.org/2010/07/another-regulatory-milestone-the-federal-register-act-turns-75.html (дата обращения: 18.10.2014).

3 *McKinney R.J.* A Research Guide to the Federal Register and the Code of Federal Regulations. P. 10 [Электронный ресурс] // Law Library Lights. URL: http://www.llsdc.org/assets/sourcebook/fall02.pdf (дата обращения: 18.10.2014).

4 *Relyea H.C.* The Federal Register: Origins, Formulation, Realization and Heritage [Электронный ресурс] // Office of the Federal Register. URL: http://www.ofr.gov/documents/FedReg_speech.pdf (дата обращения: 18.10.2014).

5 Ibid. P. 4.

6 Ibid. P. 5.

7 U.S. Code. Title 44. Chapter 15. Federal Register and Code of Federal Regulations. § 1501–1511 [Электронный ресурс] // Legal Information Institute. URL: http://www.law.cornell.edu/uscode/text/44/chapter-15 (дата обращения: 18.10.2014).

8 *McKinney R.J.* Op. cit. P. 10.

9 Federal Register Act of 1935, § 1505 [Электронный ресурс] // The U.S. National Archives and Records Administration. URL: http://www.archives.gov/federal-register/laws/federal-register/1505.html (дата обращения: 18.10.2014); U.S. Code. Title 44. Chapter 15. Federal Register and Code of Federal Regulations. § 1505 [Электронный ресурс] // Legal Information Institute. URL: https://www.law.cornell.edu/uscode/text/44/1505 (дата обращения: 18.10.2014).

10 The Federal Register. March 14, 1936 – March 14, 2006: A brief history commemorating the 70th Anniversary of the publication of the first issue of the Federal Register. P. 5 [Электронный ресурс] // The U.S. National Archives and Records Administration. URL: http://www.archives.gov/federal-register/the-federal-register/history.pdf (дата обращения: 18.10.2014).

11 Ibid.

12 Ibid.

[13] Ibid. P. 6.

[14] Administrative Procedure Act of 1946, § 552, Sec. A [Электронный ресурс] // The U.S. National Archives and Records Administration. URL: http://www.archives.gov/federal-register/laws/administrative-procedure/552.html (дата обращения: 18.10.2014).

[15] *McKinney R.J.* Op. cit. P. 10–12.

[16] Federal Property and Administrative Services Act of 1949. Title 1. Sec. 101 [Электронный ресурс] // U.S. Senate Committee on Environment & Public Works. URL: http://www.epw.senate.gov/fpasa49.pdf#search='Federal%20Property%20and%20Administrative%20Services%20Act' (дата обращения: 28.10.2014).

[17] The Federal Register. March 14, 1936 – March 14, 2006. P. 7.

[18] Ibid. P. 11.

[19] Ibid. P. 8.

[20] Public and Private Laws [Электронный ресурс] // The U.S. National Archives and Records Administration. URL: http://www.archives.gov/federal-register/laws/index.html (дата обращения: 28.10.2014).

[21] Privacy Act Issuances [Электронный ресурс] // The U.S. National Archives and Records Administration. URL: http://www.archives.gov/federal-register/publications/privacy-act.html (дата обращения: 28.10.2014).

[22] Federal Register Bulletin: The Newsletter of the Office of the Federal Register [Электронный ресурс] // The U.S. National Archives and Records Administration. URL: http://www.archives.gov/federal-register/write/newsletter/previous.html (дата обращения: 28.10.2014).

[23] The Federal Register. March 14, 1936 – March 14, 2006. P. 11.

[24] Government Printing Office Electronic Information Access Enhancement Act of 1993. § 4101 [Электронный ресурс] // U.S. Government Publishing Office. URL: http://www.gpo.gov/fdsys/pkg/BILLS-103s564es/pdf/BILLS-103s564es.pdf (дата обращения: 28.10.2014); U.S. Code. Title 44. Chapter 41. Access to Federal Electronic Information. § 4101 [Электронный ресурс] // Legal Information Institute. URL: https://www.law.cornell.edu/uscode/text/44/4101 (дата обращения: 28.10.2014).

[25] The Federal Register. March 14, 1936 – March 14, 2006. P. 16.

[26] Legal Status [Электронный ресурс] // Federal Register 2.0. URL: https://www.federalregister.gov/policy/legal-status (дата обращения: 28.10.2014).

[27] *McDonald F.* At the Federal Register, Tending to the Details of Democracy (Prologue. 2004. Vol. 36. № 3) [Электронный ресурс] // The U.S. National Archives and Records Administration. URL: http://www.archives.gov/publications/prologue/2004/fall/fed-reg.html (дата обращения: 28.10.2014).

[28] Federal Register Pamphlet [Электронный ресурс] // The Office of Federal Register. URL: http://www.ofr.gov/documents/FR-Pamphlet.pdf (дата обращения: 28.10.2014).

[29] Ibid.

Рецензии

С.Т. Петров

Борисов М.А., Романов О.А.
Основы организационно-правовой
защиты информации.
4-е изд. М.: Либроком, 2015. 248 с.

Вышедшая уже четвертым изданием книга Михаила Борисова и Олега Романова, одних из опытнейших и авторитетнейших специалистов в области защиты информации, стала бестселлером и уже исчезла из большинства магазинов. Тому есть несколько причин: все возрастающий интерес к вопросам защиты информации, повышение роли организационного и человеческого фактора в информационной безопасности, личный практический опыт и педагогическое мастерство авторов.

Книга начинается афоризмом Виктора Коняхина: «Конец информации – это конец света». Общее содержание книги исчерпывающе отражено в авторском введении, которое приведено ниже.

В настоящее время при решении задач защиты конфиденциальной информации в органе государственной власти, на предприятии, в коммерческой организации или в учреждении наиболее значимую роль играют меры организационного характера, способные по своей сути объединить в комплексе все имеющиеся способы и методы защиты информации на основе действующих норм и правил.

Это обусловлено, прежде всего, вполне объяснимым стремлением руководителей организаций и предприятий создать и на необходимом уровне поддерживать эффективную систему защиты информации, способную в каждом конкретном случае, с учетом специфики деятельности предприятия, определить необходимую совокупность сил и средств, а также мероприятий, используемых при решении задач по защите информации.

Организаторские функции руководителей предприятия играют важную роль в достижении основных целей его деятельности. Неслучайно выбор управленческих решений не может быть эффективным без строгой системы применения нормативно-мето-

дических документов на основе опыта работы предприятия в той или иной области, в нашем случае – в области, связанной с защитой конфиденциальной информации.

Многообразие функций и задач, решаемых предприятиями различных сфер деятельности и организационно-правовых форм, требует постоянного совершенствования системы защиты конфиденциальной информации, принятия новых нормативных актов, методических документов, инструкций и руководств для работников предприятия.

Объединить в себе всю имеющуюся информацию по вопросам защиты конфиденциальной информации, четко определить направления ее защиты и расставить в нужный момент приоритеты в использовании необходимых сил и средств, способов и методов ее защиты – приоритетная задача организационной составляющей системы защиты конфиденциальной информации.

Для решения данной задачи необходимы разносторонние знания нормативно-правовых основ защиты информации, направлений деятельности предприятий, очередности и порядка принятия управленческих решений в зависимости от выбранного комплекса мероприятий.

В данном учебном пособии раскрываются организационные и правовые основы защиты конфиденциальной информации, основные принципы, силы, средства, условия, направления деятельности руководителей предприятия по организации защиты конфиденциальной информации, а также дается краткая история возникновения органов защиты информации.

Книга состоит из 11 небольших глав: от исторического очерка органов защиты информации и концептуальных основ информационной безопасности до проведения служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений. Кроме того, пособие содержит несколько разнообразных и полезных приложений, охватывающих как нормативно-правовые документы, так и практические рекомендации, например по общению с представителями СМИ.

Учебное пособие предназначено для студентов, обучающихся по специальностям «Математические методы и программное обеспечение защиты информации», «Информационная безопасность», «Защита информационных технологий», «Обеспечение защиты информации в автоматизированных системах военного назначения». Рекомендуется для изучения руководителям и специалистам по информационным технологиям и защите информации коммерческих структур.

После ознакомления с данным учебным пособием нам вспомнился еще один афоризм того же автора: «Правда всегда одна. Поэтому вокруг так много шпионов».

Безусловно, вопросы организационных рисков информационной безопасности найдут свое место в учебной и научной работе ИИНТБ РГГУ, будут отражены в статьях нашего «Вестника».

О.А. Козлов

Малюк А.А. Анализ и прогнозирование потребности в специалистах по защите информации. М.: Горячая линия – Телеком, 2014. 212 с.

В монографии отмечается, что обеспечение информационной безопасности и борьба с киберпреступностью и кибертерроризмом являются важнейшими задачами современности. Оказать существенное противодействие росту преступлений в сфере информационных технологий может грамотная политика подготовки национальных кадров в сфере информационной безопасности. Эффективное решение проблем информационной безопасности на научной основе требует высокоорганизованного кадрового обеспечения, т. е. регулярной подготовки, переподготовки и повышения квалификации требуемого числа специалистов, обладающих достаточным объемом знаний и навыков. Именно поэтому в Доктрине информационной безопасности Российской Федерации, утвержденной президентом страны в 2000 г., развитие системы подготовки кадров, занятых в области обеспечения информационной безопасности, отнесено к числу первоочередных мероприятий по реализации государственной политики в сфере национальной безопасности.

Совет безопасности Российской Федерации постоянно отслеживает и обновляет направления перспективных исследований в области обеспечения информационной безопасности страны. В утвержденном в 2008 г. секретарем Совета безопасности перечне приоритетных направлений исследований в качестве трех основных разделов наряду с научно-техническими и гуманитарными выделены проблемы кадрового обеспечения информационной безопасности. Среди этих проблем одну из ведущих позиций занимает прогнозирование потребности в специалистах различного уровня и профиля.

Сложившаяся система подготовки специалистов по защите информации в основном обеспечивает прогрессивные пропорции в их воспроизводстве по различным уровням квалификации. В последнее время уменьшилось различие между максимальным и минимальным уровнями высшего образования по субъектам Российской Федерации, что позволяет говорить о последовательном процессе сглаживания неравномерности в уровне насыщенности специалистами с высшим образованием в территориальном разрезе.

В то же время, несмотря на постоянно принимаемые меры по развитию системы высшего и среднего профессионального образования, еще имеются серьезные недостатки в организации подготовки, трудоустройства и использования специалистов. Основной причиной этого является отсутствие должной обоснованности формирования государственного заказа и заявок негосударственного сектора экономики на специалистов, что обусловлено недочетами при планировании их подготовки и использования.

Планы работы системы подготовки кадров должны быть направлены на наиболее полное удовлетворение потребности отраслей и регионов в специалистах. В настоящее время, когда все усилия направлены на переход к инновационной экономике, проблема определения потребности и совершенствования управления процессом кадрового обеспечения приобретает особую актуальность.

При написании книги автором использован забытый в настоящее время опыт Советского Союза, его личный опыт работы в Министерстве высшего и среднего специального образования СССР в 1974–1985 гг., а также материалы исследований проблемы подготовки кадров, проводившихся в тот период в ведущих вузовских центрах страны, в том числе и внесшей большой вклад украинской школы под руководством профессора А.В. Головача.

В монографии освещен широкий круг методологических, методических и практических вопросов анализа и прогноза потребности в специалистах с высшим образованием в области обеспечения безопасности современных информационных технологий.

Большое внимание уделено теории и практике формирования системы показателей для оценки масштабов подготовки, регионального и отраслевого использования специалистов, прогноза потребности в них различных секторов и сфер экономики.

Предлагаемые в книге подходы носят общеметодологический характер и с успехом могут быть применены также для исследования проблем кадрового обеспечения в других отраслях экономики.

С.Т. Петров

НАЦИОНАЛЬНЫЙ ФОРУМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «ИНФОФОРУМ–2015»

5–6 февраля 2015 г. в Москве состоялся очередной, XVII Национальный форум информационной безопасности «Инфофорум–2015». Традиционно именно Инфофорум открывает календарь наиболее значимых событий года в области информационной безопасности.

Прежде чем перейти к описанию мероприятий нынешнего года, стоит немного рассказать о причинах его появления и принципах работы.

Форум проводится с 2001 г., инициаторами его проведения выступили Аппарат Совета безопасности Российской Федерации и Комитет Государственной думы Российской Федерации по безопасности. Инфофорум стал первым отечественным мероприятием в сфере информационной безопасности и за время своего существования превратился в знаковое событие отрасли.

Появление Инфофорума предопределило время, ведь, как известно, XXI век – век информации. Россия нуждалась в новой дискуссионной площадке, способной консолидировать экспертное сообщество, бизнес и государство для определения направлений развития информационного общества и решения проблем информационной безопасности. Такой площадкой и стал Инфофорум.

Всего лишь десятилетие назад проблематика информационной безопасности представляла интерес преимущественно для узкого круга специалистов. С развитием информационно-коммуникационных технологий вопросы информационной безопасности приобрели значение для массовой аудитории. Инфофорум из узкоспециального мероприятия превратился в масштабный всероссийский форум, в рамках которого проходит обсуждение широкого спектра технологических и гуманитарных проблем обеспечения информа-

ционной безопасности, вырабатываются предложения по формированию государственной политики в этой сфере, анализируется практика правоприменения, демонстрируются новые российские и зарубежные решения.

Аудиторию Инфофорума составляют специалисты, работающие во всех отраслях экономики, представляющие органы федеральной и региональной власти, местного самоуправления, науку, образование, бизнес.

Сегодня Инфофорум – это целый ряд мероприятий, посвященных различным аспектам информационной безопасности: Национальный форум информационной безопасности «Инфофорум», Евразийский форум информационного взаимодействия «Инфофорум-Евразия», международная конференция «Доверие и безопасность в информационном обществе», которая проводится за рубежом, всероссийские тематические конференции по электронному документообороту и электронному образованию, региональной безопасности, безопасности в Интернете, а также круглые столы, профессиональные конкурсы и премии.

Важный аспект деятельности Инфофорума – привлечение внимания широкой общественности к проблематике информационной безопасности и защиты информации. Так, Инфофорум является инициатором и организатором ежегодной Всероссийской акции «Информационная безопасность для всех», которая проходит при поддержке Министерства связи и массовых коммуникаций РФ, Общественной палаты РФ и при участии образовательных учреждений и других организаций из всех регионов России.

Отличительной чертой деятельности Инфофорума является то, что с момента основания в нем активно участвуют как коммерческие компании, так и органы государственной власти, правоохранительные органы, силовые ведомства.

Мероприятия Инфофорума проводятся при организационной поддержке Совета безопасности РФ, Комитета по безопасности и противодействию коррупции Государственной думы РФ, МИД России, ФСБ России, ФСТЭК России, Правительства Москвы и многих других федеральных и региональных ведомств.

Среди партнеров Инфофорума – крупные российские и международные ИТ-компании: ГК Ростехнологии, Техносерв, КРОК, Ай-Теко, ВСС, АйТи, Microsoft, IBM, Oracle, Huawei.

Такое многостороннее сотрудничество, осуществляемое в рамках Инфофорума, предоставляет уникальную возможность для взаимодействия бизнеса и государства. Инфофорум дает представителям ИТ-сектора экономики возможность выйти со своими

инициативами и предложениями на самый высокий уровень, а государству, в свою очередь, быть в курсе последних ИТ-тенденций, понимать, чем живет ИТ-бизнес в России, какие существуют проблемы, достижения и перспективы.

По итогам мероприятий Инфофорума принимаются резолюции и другие итоговые документы, содержащие выводы и предложения по развитию отрасли информационной безопасности и ее законодательному регулированию. Рекомендации Инфофорума направляются в Правительство РФ, становятся основанием для предложений по совершенствованию законодательства в сфере защиты информации, персональных данных, доступа к информации, внедрения электронных сервисов для граждан.

За время работы Инфофорум создал и сплотил вокруг себя сообщество авторитетных экспертов в области информационной безопасности, которые принимают конкретные решения, определяющие настоящее и будущее отрасли в нашей стране. По сути, Инфофорум сегодня, в отсутствие специализированного органа, отвечающего за информационную безопасность в Российской Федерации, выполняет функцию межведомственного и межинституционального координатора усилий различных структур по развитию отрасли информационной безопасности и укреплению информационных рубежей государства.

В работе Инфофорума активно участвует молодежь – старшеклассники, студенты, аспиранты.

* * *

В этом году, как и прежде, Инфофорум проводит свою работу в здании Правительства Москвы на Новом Арбате, что позволяет с высоким техническим оснащением и комфортно проводить масштабные пленарные заседания, на которые приглашаются более тысячи человек, и многочисленные секции.

Работа форума открылась пленарным заседанием, темой которого стала информационная безопасность России в условиях глобального информационного общества. Вопросами для обсуждения стали:

– глобальные риски в сфере информационной безопасности для России, стран ЕАЭС, ОДКБ, ШОС и других стран. Задачи формирования государственной политики в сфере обеспечения информационной безопасности Российской Федерации в новых политических условиях;
– обеспечение информационной и технологической независимости: приоритетные направления развития отечественной

науки, техники, образования, задачи развития информационной инфраструктуры, организация экономической поддержки российских компаний и специалистов, работающих в сфере информационной безопасности, поиска альтернативных технологических решений и продуктов;
- задачи правового регулирования Интернета в целях создания пространства доверия на территории Российской Федерации и Евразии;
- роль и задачи бизнес-сообщества и гражданского общества по обеспечению безопасности критической информационной структуры Российской Федерации;
- электронные услуги населению, защищенный электронный документооборот и электронная подпись: нерешенные проблемы;
- национальная платежная система и вопросы информационной безопасности в кредитно-финансовой сфере;
- информационное противоборство и электронные СМИ: гуманитарные вопросы информационной безопасности.

Среди выступающих: С.С. Суворов, заместитель начальника Генерального штаба Вооруженных сил; А.В. Крутских, специальный представитель Президента России по вопросам международного сотрудничества в области информационной безопасности, посол по особым поручениям; Д.Г. Грибков, начальник Департамента обеспечения безопасности в области информации и информационных технологий аппарата Совета безопасности; А.Н. Мошков, начальник Бюро специальных технических мероприятий МВД России; Н.Н. Мурашов, представитель научно-технической службы ФСБ России и др.

Тематическая работа форума проходила по секциям:
- устойчивость и безопасность российского сегмента сети Интернет;
- доверенная информационная среда: мониторинг обеспечения информационной безопасности и поиск альтернативных решений;
- инфраструктура финансово-кредитной системы Российской Федерации: вопросы информационной безопасности;
- информационная безопасность перспективных технологий. Тенденции-2015;
- безопасный город и безопасность критической информационной инфраструктуры;
- электронные услуги и юридически значимый электронный документооборот: проблемы и решения;

– стандарты новых знаний: актуальные задачи подготовки кадров для отрасли информационной безопасности.

Уже несколько лет на Инфофоруме представлена секция, посвященная гуманитарным проблемам информационной безопасности. Его сопредседателем является А.А. Тарасов, неизменный член оргкомитета форума, проф., д-р техн. наук, директор ИИНТБ РГГУ. В этом году тематика секции была обозначена как «Информационное общество: информационная культура и информационное противоборство».

Среди обсуждаемых групп вопросов:

– «информационное оружие» – реальные угрозы для безопасности государств, общества и граждан, их частной и интеллектуальной собственности в цифровую эпоху;
– электронные СМИ и «электронная» личность: новые угрозы и вызовы гуманитарного характера. Взгляд российских и зарубежных специалистов;
– социально-психологические аспекты информационной безопасности для различных слоев населения, социальная инженерия как метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека;
– подходы и методы формирования и укрепления у граждан навыков безопасного поведения в информационной сфере;
– создание системы информационно-консультативной помощи в области предупреждения угроз безопасности использования общедоступных и корпоративных информационных систем, а также ликвидации последствий проявления угроз в информационной сфере;
– проблемы формирования этических норм в области информационно-телекоммуникационных взаимодействий, развития профессиональных правил и стандартов безопасного использования информационных и телекоммуникационных технологий;
– программы развития культуры информационной безопасности, информирования граждан о сущности и потенциальных опасностях информационных технологий, механизмы защиты пользователя от агрессии информационной среды;
– информационная безопасность культуры – информационные активы, угрозы и риски, информационная безопасность культурных ценностей, учреждений культуры и интернет-проектов в сфере культуры.

С некоторыми подходами по последней группе вопросов можно ознакомиться в статье «Формирование системы обеспечения информационной безопасности Российской Федерации в сфере культуры», публикуемой в настоящем издании. Среди докладов секции можно выделить «Образование как сфера информационного противоборства. Формирование культуры информационной безопасности» (А.А. Малюк) и «Музейная безопасность в формате 5D» (А.Н. Ненашев). Основные положения этих докладов будут опубликованы в следующих номерах «Вестника».

В текущем году пройдет еще три мероприятия Инфофорума: во Владивостоке (июль), Томске (сентябрь), Алматы (Казахстан, октябрь).

Сайт Инфофорума: www.infoforum.ru

Abstracts

Yu. Kalinina

FORMATION OF TECHNICAL LEAKAGE CHANNEL OF VOICE INFORMATION IN NETWORKS BASED ON FIBER-OPTIC TECHNOLOGY

This article talks about the existing and applied in real time networks based on fiber-optic technology and provides a definition, as well as a description of forming the technical leakage channel of voice information in networks based on fiber-optic technology.

Key words: fiber-optic technology, voice information, technical leakage channels.

V. Kazarin, R. Sharyapov

MALWARE NEW GENERATION – ONE OF THE MAJOR THREATS TO INTERNATIONAL INFORMATION SECURITY

Analysis of the events of the last 3–4 years, says that the era of cyber-warfare has begun. Development and application of such malicious programs like Stuxnet, Flame, Duqu, etc. allows us to conclude that the large-scale sabotage and reconnaissance cyber operations (if not the cyber war) conducted by government agencies against critical facilities of other countries started. And this in itself may be a harbinger of cyberwar. Nature, characteristics of such cyber operations and related problems, as well as malware developed for that are the subject of this article.

The solution of problems of detection and neutralization of malware should be carried out as in the national systems for combating cyberattacks, and in the system of international information security able to solve such problems in politic, diplomatic, legal, technological and organizational areas. Suggestions on measures to be taken in the context of initiation of such system and its evolving are also considered in the present work.

Key words: cyberspace, cyber-warfare, information and communication technologies, information weapons, malware, international information security.

E. Khalepa

EXPERIENCE IN DOCUMENTING OF ACTIVITIES FOR PROVIDING OF INTELLECTUAL PROPERTY PROTECTION IN MOSCOW ENTREPRENEURSHIP IN THE XIXth AND EARLY XXth CENTURIES

The article deals with the issues of inventions use in business of joint-stock companies in Russia in the XIXth and early XXth centuries. The role of a privilege as a title of protection for an invention is also considered. The article analyses the procedure of execution of documents for obtaining of privileges, registration of trademarks, manufacturing patterns and products.

Key words: Joint-stock company, the Moscow entrepreneurship, intellectual property protection, documentation, execution of privileges for an invention, registration of trademarks and manufacturing patterns.

V. Konyavskiy, I. Nazarov, S. Petrov, A. Tarasov

THE FORMATION OF THE SYSTEM OF MAINTENANCE FOR INFORMATION SECURITY OF THE RUSSIAN FEDERATION IN THE SPHERE OF CULTURE

This article discusses an integrated approach to information security in the sphere of culture. Based on the analysis of subject domain and examination of cultural institutions main problems and difficulties in developing information security systems are identified. The concept of information security, estimation technique for the evaluation of information assets, risks and threats, other techniques and a set of information security policies, road map are presented. The proposed documents for the first time highlight main conceptual and practical approaches to building system of information security culture generally and in individual cultural institutions.

Key words: culture, cultural values, information security, information assets, risks and threats.

V. Lobastov

PROTECTION OF CONFIDENTIAL CONVERSATIONS IN THE CAR USING VIBRO-ACOUSTIC EMITTERS

The article analyses main drawbacks in the known methods of active protection of confidential conversations in the car and proposes a new promising method of protection using vibro-acoustic emitters. The publication presents descriptions of proposed perspective method, its principles and two implementation schemes. In addition, to assess the effectiveness of the proposed method, the article presents the results of experiments, carried out using special equipment to intercept the acoustic information in a simulation of the confidential talks in the car with protection through the proposed method.

Key words: acoustic information protection, acoustic protection, protection of confidential conversations in the car, the system of protection of conversations.

A. Pestryaev, L. Voronova, V. Voronov

DESIGNING MULTI-AGENT SYSTEM TO COLLECT TEXTUAL INFORMATION FROM THE NETWORK

The article considers designing of multi-agent system MAS “Stop TSD”, which collects links from the Internet. The system is designed to search for banned words and phrases in the pages of social networking services. Ontology contains words and expressions of terrorism, suicide and drugs (TSD).

Designing of the system agents, databases, access mechanisms in the global network was carried out and MAS “Stop TSD” system was realized. Its testing was accomplished. By now the system has collected more than 10,000 links to pages containing “dangerous” information.

MAS takes into account the projected multi-core computer architecture, analysing the size of the cache and distributing agents working on different processor cores. The work was done using the package of later information technologies such as “Qt Creator v. 4.7.4”, “MSSQL Server 2012”, “Boost C++ Libraries v.1.53”.

The advantages of the developed system, as compared with existing specific examples discussed.

Key words: multiagent system, MAS, malicious information, CPU cache memory, multi-core computer architecture, suicide, terrorism, drugs.

A. Rabinovich

USER AUTHENTICATION METHOD WITH TSM-SERVICE AS A TRUSTED ELEMENT OF NFC-SYSTEM

This article describes the method of interactive user authentication with TSM service as a trusted element of NFC-system. To this end it is suggested that already available roles of TSM operator, namely those of known safe data exchange as well as exchange of control keys for safe access to applications are to be complemental with key management role for user authentication in NFC-system as an analog of public key certificate management in PKI-infrastructure.

Key words: user authentication, near field communication, mobile operator, public key certificate.

E. Sidorenko

THE ROLE OF DOCUMENTS IN QUALITY MANAGEMENT SYSTEM

This article is about some key points of quality management system regarding working with documents. Particular attention is paid to the value of documentation in quality management, an attempt is made to define a new role of documents in management through the analysis of the requirements for the composition and structure of documents in the state as well as in commercial organizations. The factors influencing the effectiveness of documents as a tool for quality management is identified.

Key words: document, quality management system, regulation, quality, documented procedures.

V. Stepanov

THE OFFICE OF THE FEDERAL REGISTER IN THE STRUCTURE OF THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. HISTORY AND ITS ROLE IN PUBLIC REGULATION

The article considers the historical development, purpose and role of the most important structural unit of The National Archives and Records Administration of the USA, namely The Office of the Federal Register; provides a detailed description of the history of the formation

of the Office and its legal status; shows the level of Office's participation in political process.

Key words: Federal Register, publications, documents, legislation.

V. Zapechnikov

THE DEVELOPMENT OF THE SOFTWARE PACKAGE FOR ANALYTICAL, NUMERICAL AND SIMULATION MODELING OF QUEUEING SYSTEMS

The article is about the development of software package for modeling of queuing systems. The feature of the software system is that it allows modeling many kinds of queuing systems, starting from the elementary systems and including far more complex ones. For each type of systems analytical (or numerical) and simulation modeling can be spent. Comparison of the results obtained by means of completely different techniques allows ensuring that the models are adequate. The main areas of application for the software package are calculation and prediction of availability, reliability, fault tolerance and performance measures of complex data processing systems, including cloud-based technologies.

Key words: queueing systems, analytical modeling, simulation, availability, performance measures.

A. Zaytsev, A. Malyuk

SYSTEM DYNAMICS MODELING OF THREAT OF INTELLECTUAL PROPERTY THEFT

An insider threat classification is adduced, method of insider threats' countermeasure decision-making support using system dynamics modeling is considered and forecasting behavioral models for threats of theft of intellectual property for business advantages alone and with accomplices are developed.

Key words: system dynamics, behavioral models, imitation modeling, insider intruder, intellectual property.

Сведения об авторах

Воронов Вячеслав Игоревич – кандидат технических наук, доцент кафедры информационных систем и моделирования ИИНТБ РГГУ, vorvi@mail.ru

Воронова Лилия Ивановна – доктор физико-математических наук, профессор, заведующая кафедрой информационных систем и моделирования ИИНТБ РГГУ, voronova2001@mail.ru

Зайцев Антон Сергеевич – аспирант Национального исследовательского ядерного университета «МИФИ», Anthony.Zaytsev@gmail.com

Запечников Сергей Владимирович – доктор технических наук, доцент, профессор кафедры информационной безопасности банковских систем Национального исследовательского ядерного университета «МИФИ», SVZapechnikov@mephi.ru

Казарин Олег Викторович – доктор технических наук, ведущий научный сотрудник Института проблем информационной безопасности МГУ им. М.В. Ломоносова; старший научный сотрудник ИИНТБ РГГУ, okaz2005@yandex.ru

Калинина Юлия Дмитриевна – аспирант ИИНТБ РГГУ, abarakedavra@gmail.com

Козлов Олег Александрович – доктор педагогических наук, профессор, заместитель директора Института информатизации образования Российской академии образования

Конявский Валерий Аркадьевич – доктор технических наук, профессор Московского физико-технического института; научный руководитель Всероссийского научно-исследовательского института проблем вычислительной техники и информатизации

Лобастов Вячеслав Игоревич – аспирант ИИНТБ РГГУ, nuar@bk.ru

Малюк Анатолий Александрович – кандидат технических наук, профессор Национального исследовательского ядерного университета «МИФИ»; профессор Финансового университета при Правительстве Российской Федерации, AAMalyuk@mephi.ru

Назаров Игорь Григорьевич – кандидат технических наук, генеральный директор ЗАО «ОКБ САПР», ig_nazarov@okbsapr.ru

Пестряев Александр Андреевич – ведущий программист отдела «Коммуникационное программное обеспечение» ЗАО «Сетевые Технологии», aleksandrpestr@rambler.ru

Петров Сергей Томасович – старший научный сотрудник ИИНТБ РГГУ, 5008604@gmail.com

Рабинович Анастасия Сергеевна – аспирант ИИНТБ РГГУ, jilly_s@mail.ru
Сидоренко Елена Валерьевна – аспирант ИАИ РГГУ; специалист по взаиморасчетам компании «Панальпина», prelude28@mail.ru
Степанов Владислав Александрович – аспирант, сотрудник Российского государственного архива научно-технической документации, специалист I категории, tomin1991@yandex.ru
Тарасов Александр Алексеевич – доктор технических наук, профессор, директор ИИНТБ РГГУ, aa_tarasov@list.ru
Халепа Екатерина Анатольевна – аспирант кафедры истории и организации архивного дела ИАИ РГГУ, e_eremeeva@bk.ru
Шаряпов Ринат Абдулберович – кандидат политических наук, заведующий отделом Института проблем информационной безопасности МГУ им. М.В. Ломоносова, SharyapovR@iisi.msu.ru

General data about the authors

Kalinina Yuliya D. – postgraduate student, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, abarakedavra@gmail.com

Kazarin Oleg V. – Dr. in Engineering, leading researcher, Institute for Information Security Issues, Lomonosov Moscow State University; senior researcher, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, okaz2005@yandex.ru

Khalepa Ekaterina A. – postgraduate student, Department of History and Organisation of Archives, Institute for History and Archives, Russian State University for the Humanities, e_eremeeva@bk.ru

Konyavskiy Valeriy A. – Dr. in Engineering, professor, Moscow Institute of Physics and Technologies; scientific supervisor, All-Russian Scientific Research Institute of Problems of Computer Technologies and Informatics

Kozlov Oleg A. – Dr. in Redagogics, professor, deputy director, Institute of Informatization of Education of the Russian Academy of Education

Lobastov Vyacheslav I. – postgraduate student, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, nuar@bk.ru

Malyuk Anatoliy A. – Ph.D. in Engineering, professor, National Research Nuclear University "MEPhI"; professor, Financial University under the Government of the Russian Federation, AAMalyuk@mephi.ru

Nazarov Igor G. – Ph.D. in Engineering, director general, CJSC "OKB SAPR Ltd", ig_nazarov@okbsapr.ru

Pestryaev Alexandr A. – leading programmer, Communications Software Department, CJSC "NetWork Technologies Ltd.", aleksandrpestr@rambler.ru

Petrov Sergey T. – senior researcher, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, 5008604@gmail.com

Rabinovich Anastasia S. – postgraduate student, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, jilly_s@mail.ru

Sharyapov Rinat A. – Ph.D. in Politics, Department head, Institute for Information Security Issues, Lomonosov Moscow State University, SharyapovR@iisi.msu.ru

Sidorenko Elena V. – postgraduate student, Institute for History and Archives, Russian State University for the Humanities; settlement specialist, "Panalpina" Company, prelude28@mail.ru

Stepanov Vladislav A. – postgraduate student, co-worker, Russian State Archives of Scientific and Technical Documentation, I category specialist, tomin1991@yandex.ru

Tarasov Aleksandr A. – Dr. in Engineering, professor, director, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, aa_tarasov@list.ru

Voronov Vyacheslav I. – Ph.D. in Engineering, associate professor, Department of Information Systems and Modeling, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, vorvi@mail.ru

Voronova Liliya I. – Dr. in Physics and Mathematics, professor, head, Department of Information Systems and Modeling, Institute for Information Sciences and Security Technologies, Russian State University for the Humanities, voronova2001@mail.ru

Zapechnikov Sergey V. – Dr. in Engineering, associate professor, professor, Department of Information Security of Banking Systems, National Research Nuclear University "MEPhI", SVZapechnikov@mephi.ru

Zaytsev Anton S. – postgraduate student, National Research Nuclear University "MEPhI", Anthony.Zaytsev@gmail.com

Заведующая редакцией *И.В. Лебедева*

Художник *В.В. Сурков*

Художник номера *В.Н. Хотеев*

Корректор *О.К. Юрьев*

Компьютерная верстка *Н.В. Москвина*

Формат 60×90 1/16.
Усл. печ. л. 10,8. Уч.-изд. л. 11,3.
Тираж 1050 экз. Заказ № 69

Издательский центр
Российского государственного
гуманитарного университета
125993, Москва, Миусская пл., 6
www.rggu.ru
www.knigirggu.ru