СПРАВОЧНО-ИНФОРМАЦИОННЫЙ РАЗДЕЛ

УДК 005.745:004.056

В.В. Арутюнов

Об итогах Второй международной научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра»

Рассматриваются итоги состоявшейся в Российском государственном гуманитарном университете (РГГУ) конференции, на которую было представлено более 40 докладов и где функционировали три секции: Общие вопросы обеспечения информационной безопасности, Программно-аппаратные методы и средства защиты информации, Практика и перспективы развития направлений информационной безопасности. Приводится краткий обзор основных пленарных и секционных докладов.

Ключевые слова: *информационная безопасность, защита информации, информационные технологии, программные средства защиты, информационные системы, аппаратные средства защиты, система защиты информации*

В апреле 2019 г. в Российском государственном гуманитарном университете (РГГУ) проводилась Вторая международная научно-практическая конференция «Информационная безопасность: вчера сегодня, завтра», в которой приняли участие более 120 учёных и специалистов, было представлено более 40 докладов и функционировали три секции: Общие вопросы обеспечения информационной безопасности, Программно-аппаратные методы и средства защиты информации, Практика и перспективы развития направлений информационной безопасности.

Основная цель конференции – обеспечение эффективного взаимодействия между разработчиками и потребителями различной продукции в сфере информационной безопасности для ускорения продвижения современных технологий на рынке систем и средств безопасности, а также широкий обмен научными знаниями и опытом между специалистами, работающими в различных сферах защиты информации.

О широте и глубине обсуждавшихся проблем в определённой мере свидетельствуют не только названия секций конференции, но и тематика докладов.

Приведём краткий обзор основных пленарных и секционных докладов, представляющих интерес для отечественных и зарубежных специалистов в области информационной безопасности.

В докладе д.т.н. В.И. Королева (Федеральный исследовательский центр «Информатика и управление» РАН) **"Факторы трансформации парадигмы безопасности информационных систем цифровой экономики"** были представлены информационные системы (ИС) цифровой трансформации экономической деятельности как компоненты предметных экосистем, под которыми понимается некоторая сеть (партнёрство) организаций, где данные в цифровой форме являются ключевым фактором во всех сферах социально-экономической деятельности и обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан.

Автор отмечает, что погружение экосистемы цифровой экономики в киберпространство и широкое использование средств цифровых технологий вызывает новую проблемную ситуацию в понимании обеспечения безопасности. Эту проблемную ситуацию можно разделить на два блока вопросов: первый – относится непосредственно к обеспечению и поддержке в цифровой среде определённого уровня свойств самой информации и учёта её влияния на систему; второй – связан с характером функционирования открытых распределённых ИС в киберпространстве, с новыми архитектурными решениями в области информационных технологий и с широким применением цифровых технологий в экономике деятельности.

Докладчик анализирует новые вызовы и факторы влияния на обеспечение безопасности информационных систем цифровой экономики.

Доклад д.т.н. А.П. Фисуна (Орловский государственный университет им. И.С. Тургенева) и к.ю.н. Ю.А. Белевской (Среднерусский институт управления – филиал РАНХиГС при Президенте Российской Федерации) **"Развитие государственной политики в области обеспечения информационной безопасности современного общества в условиях западной информационной агрессии"** посвящен общесистемным проблемам совершенствования государственной политики в области обеспечения информационной безопасности (ИБ) информационного общества в условиях воздействия информационных угроз и агрессивной информации, оказывающим необратимые последствия на качество управленческой информации, обрабатываемой социотехническими системами с помощью информационно-телекоммуникационных технологий (ИКТ) в различных сферах и видах деятельности информационного общества (ИО), а также разрушающие воздействия на человека, его психологическое состояние, нравственные, политические и иные ценности и, в целом, на общество и государство.

В числе этих проблем сложность определения самого общего и собирательного понятия «Запад», широкое использование ИКТ как основополагающего базиса существования и развития деятельности во все сферах и видах ИО, двойственность и противоречивость функционального предназначения средств массовой коммуникации и массовой информации, недостаточность подготовки специалистов в политико-правовой сфере ИО в области обеспечения ИБ государственной политики ИО и ряд других.

Акцентируется внимание на развитии эффективной системы подготовки специалистов в области обеспечения ИБ политической сферы ИО, способных решать задачи обеспечения ИБ, связанные не только с традиционными видами и направлениями в политологии, но и с учетом новых видов угроз ИО на основе единых государственных образовательных стандартов с региональными и ведомственными компонентами, где общеметодологические положения и части программ не должны быть разноплановыми.

В докладе к.ист.н. Г.А. Шевцовой (Российский государственный гуманитарный университет – РГГУ) **«О результативности научно-исследовательской работы Института информационных наук и технологий безопасности Российского государственного гуманитарного университета»** на примере данного вуза анализируется результативность научно-исследовательской деятельности за последние четыре года с учетом требований, предъявляемых к вузу по проведению аккредитационной экспертизы, целью которой является подтверждение соответствия федеральным государственным образовательным стандартам образовательной деятельности по основным образовательным программам и подготовки обучающихся в образовательных организациях, а также определение соответствия содержания и качества подготовки обучающихся в учебной организации.

Одним из важнейших показателей результативности научной деятельности выступает критерий по участию в научно-исследовательской работе профессорско-преподавательского состава вуза. Образование преподавателей должно соответствовать профильности преподаваемых ими дисциплин, а в случаях отсутствия профильности учитываются результаты повышения квалификации по дисциплинам учебного плана.

Другое направление деятельности вуза в области научной работы – исследования по проблемам высшей школы, которые направлены на составление научно-методических материалов, подготовку учебников и учебных пособий, разработку рабочих учебных программ по специальным курсам, а также внедрение активных форм и проблемных методов обучения. В докладе анализируется привлечение студентов к совместным проектам, реализуемым по профилю научных интересов. Основной смысл этого направления заключается и в том, чтобы через научную работу приобщить студентов к самостоятельной работе, заинтересовать их в тематике будущих исследований и профессиональной деятельности.

Широкий спектр статистических данных по результативности научной деятельности, приводимый автором, демонстрирует в том числе достаточно устойчивую динамику подготовки научных статей в вузе с участием студентов и аспирантов.

Доклад д.т.н. С.Е. Симанова, И.В. Нестерова, И.А. Пенькова (Всероссийский научно-исследовательский институт противопожарной обороны МЧС России) **"Общие вопросы обеспечения информационной безопасности мобильных робототехнических комплексов"** посвящен рассмотрению мобильного робототехнического комплекса (РТК) как информационной системы, структурно состоящей из двух контуров – субъектов информационной защиты: во внешний контур организационно входят каналы связи (дистанционного управления, супервизорного управления и т.п.), система навигации и наведения, система технического зрения; в состав внутреннего контура входят бортовые вычислители, система управления, датчики внутреннего состояния и система энергетики.

В качестве основных средств борьбы с угрозами РТК выступают:

- применение требований входного контроля для всех поступающих комплектующих из состава электронной компонентной базы;
- соблюдение комплекса требований и норм информационной безопасности на этапе разработки, монтажа, наладки и испытаний РТК в условиях предприятия-изготовителя;
- применение проверенного (в том числе и компетентными органами) оборудования при разработке специального программного обеспечения и т.д.

Авторы отмечают, что, как показала практика, выполнение порядка и правил основных норм в области обеспечения информационной безопасности, прописанных в том числе и в ряде государственных стандартов по робототехнике, позволяет успешно минимизировать уязвимость систем РТК.

В докладе к.ф.-м.н. И.В. Башелханова, к.э.н. Н.И. Демкиной, к.т.н. С.М. Володина, к.т.н. А.В. Роя (Финансовый университет при Правительстве РФ) и д.б.н. А.В. Олескина (Московский государственный университет им. М.В. Ломоносова) **"Обеспечение информационной безопасности в киберфизических системах в условиях Индустрии 4.0"** анализируется концепция «Индустрии 4.0», которая зародилась в начале текущего десятилетия в Германии и стала копироваться в других западных странах. По замыслу авторов «Индустрии 4.0» социотехнические системы в будущем должны преобразоваться в киберфизические системы – интероперабельные системы, состоящие из цифровых компонентов и физических сущностей любого вида (включая биологические и искусственные объекты).

Анализ, выполненный докладчиками, показывает, что в последние годы развитие нормативной базы в области информационных технологий в России в целом явно отстает от требований широкого круга специалистов, занимающихся созданием и внедрением информационных систем; и для формирования национальной нормативной базы в этой сфере необходимо разработать:

1) программу создания и реализации нормативного обеспечения Государственных профилей взаимосвязи открытых систем и функциональной среды открытых систем;

2) корпоративную базу стандартов, нормативно-методических и организационно-технических документов, аппаратно-программных и инструментальных средств в области открытых систем;

3) рекомендации по стандартизации Государственного профиля функциональной среды открытых систем (профиль переносимости прикладных программ) и Государственного профиля взаимосвязи открытых систем;

4) руководство по применению Государственных профилей функциональной среды и взаимосвязи открытых систем при проектировании информационных систем, создаваемых по федеральным заказам;

5) комплект организационно-технических документов, определяющих разработку «Системы аттестационного тестирования и сертификации в области открытых информационных систем», а также Программу создания методических и технологических средств аттестационного тестирования компонентов и средств открытых информационных систем;

6) методы привлечения внебюджетных финансовых средств для проведения работ по формированию единого информационного пространства.

Доклад д.т.н. В.А. Минаева, д.т.н. М.П. Сычева (Московский государственный технический университет им. Н.Э. Баумана), д.т.н. И.Д. Королёва и к.т.н. О.В. Петровой (Краснодарское высшее военное училище им. генерала армии С.М. Штеменко) **"Модель защиты многоканальных автоматизированных комплексов от DDOS-атак" посвящен** моделированию системы защиты автоматизированных информационных систем (АИС) от DDoS-атак. В работе ставится задача распределения потока заявок в системе многоканального обслуживания с различной пропускной способностью каналов.

Для того чтобы в ходе реализации DDoS-атак на АИС избежать отказы в обслуживании потока заявок, необходимо заблаговременно реагировать на изменения этого потока, адаптивно подстраивая общую пропускную способность каналов автоматизированных комплексов. Подобным же образом возможно производить расчеты при большем числе каналов. В случае возникновения сложностей при аналитическом представлении вероятностей отказа возможно построение имитационной модели системы защиты АИС. Докладчики приводят формулы для расчета предельных вероятностей отказа системы при установившемся режиме обработки поступающих заявок.

В докладе Д.В. Чемарева (Дальневосточный юридический институт МВД России) **"Модель анализа и оценки системы защиты информации от внутреннего нарушителя"** на основе классификации внутренних нарушителей и анализа статистических данных по угрозам, совершаемым последними, рассматриваются диаграммы причинно-следственных связей и диаграммы потоков для кражи интеллектуальной собственности, отображающие взаимосвязь основных элементов, в числе которых: желание совершить кражу, осведомленность об информационной безопасности, доверие организации инсайдеру, заметание следов, желание покинуть организацию и др.

В результате была получена система уравнений, которая является основой для описания зависимостей между элементами при построении имитационных моделей в среде имитационного моделирования *AnyLogic PLE*. Апробация этих моделей позволяет подтвердить адекватность разработанных моделей и наглядно оценить систему защиты информации от внутреннего нарушителя при различных настройках. Достоверность результатов апробации обеспечивается системным учетом факторов, влияющих на решение поставленных научных задач; обоснованным выбором основных допущений и ограничений при постановке научных задач; корректным выбором характеристик и показателей, включенных в процесс моделирования; достаточно хорошим совпадением результатов имитационного моделирования с эмпирическими данными.

Доклад д.т.н. Г.М. Антоновой (Институт проблем управления РАН) **"Применение методов идентификации для обработки результатов экспериментов с имитационными моделями систем информационной безопасности"** посвящён анализу вариантов описаний результатов имитационных экспериментов, применяемых с использованием методов параметрической идентификации для определения моделей систем информационной безопасности. Автор отмечает, что полная классификация методов идентификации пока не создана.

Специальный программный пакет позволяет реализовать сравнение существующих алгоритмов идентификации в процессе обработки экспериментальных данных, полученных в блоке имитационного моделирования, и выбрать наилучший из библиотеки, включающей более 50-ти различных алгоритмов

идентификации. В состав библиотеки входят фильтр Калмана, алгоритмы Цыпкина, Айзермана, Гаусса-Ньютона и др. Проверка функционирования пакета при решении задачи определения области эффективности сложной системы по результатам применения сеточных методов равномерного зондирования показала его широкие возможности.

В процессе применения пакета возможна реализация процедуры формального выбора алгоритма идентификации по результатам решения задачи многокритериальной оптимизации, использующей критерий качества адаптации, которая характеризует величину ошибки между разными видами моделей и объектом.

В докладе д.т.н. В.В. Арутюнова и М.С. Курышевой (Российский государственный гуманитарный университет**) "О кластеризации национальных стандартов России и нормативно-правовых документов ФСТЭК в области информационной безопасности"** анализируются разработанные в России за последние 20 лет нормативно-правовые документы Федеральной службы технического и экспертного контроля России (ФСТЭК) и национальные стандарты в области информационной безопасности; на основе различных источников выявлена динамика создания и составлен полный реестр этих документов на начало 2019 г. Отмечается, что значительное число разработанных стандартов и документов в этой сфере, во-первых, свидетельствует о достаточно высоком уровне зрелости технологий, используемых в области информационной безопасности, и, во-вторых, позволяет выявить основные кластеры стандартов и документов для тех направлений исследований в сфере защиты информации, которые могут стать наиболее развивающимися и перспективными. В их числе следующие кластеры национальных стандартов: методы и средства обеспечения безопасности, форматы данных для биометрических систем защиты информации, телекоммуникации и сети.

В среде документов ФСТЭК выделяются три таких кластера: профили защиты, общие и специальные требования к защите информации, защита от несанкционированного доступа.

Доклад В.А. Гладилиной и д.т.н. С.Н. Неизвестного (Российский государственный социальный университет) **"Роль компетенции медиации руководителя службы информационной безопасности предприятия в управлении информационными рисками"** посвящен значимости компетенции медиации руководителя службы информационной безопасности, его роли в управлении информационными рисками, упреждении конфликтов. Выявлены основные причины нарушения защиты конфиденциальной информации, причины устранения и препятствования подобным инцидентам. В результате разработаны основные аспекты компетенции медиации руководителя службы информационной безопасности предприятия.

Чтобы процесс медиации прошёл на высоком профессиональном уровне, авторы доклада считают, что руководитель службы информационной безопасности должен соответствовать таким требованиям, как развитая способность эмпатии, высокий уровень *EQ* (*Emotional Quotient*), высокое владение профессиональной этикой, риторикой (в части способности адекватно доносить мысль адресату), знание основ конфликтологии, коммуникационные навыки и т.д.

Компетентность в области медиации (устранения конфликтов) является одной из важнейших у руководителя службы информационной безопасности предприятия. Формирование данной компетентности поможет значительно улучшить состояние защиты информации предприятий и вывести управление информационными рисками на более высокий профессиональный уровень.

По итогам работы конференции был издан сборник трудов её участников[1].

Материал поступил в редакцию 29.04.19.

Сведения об авторе

АРУТЮНОВ Валерий Вагаршакович – доктор технических наук, профессор Российского государственного гуманитарного университета**,** Москва
e-mail: warut698@yandex.ru

[1] Информационная безопасность: вчера, сегодня, завтра: сб. ст. Международной научно-практической конференции / под ред. В.В. Арутюнова. – М.: РГГУ, 2019. – 220 с.

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК

предлагает научным работникам, аспирантам и другим специалистам в области естественных, точных и технических наук, желающим быстро и эффективно опубликовать результаты своей научной и научно-производственной деятельности, использовать способ публикации своих работ через *систему депонирования.*

Депонирование (передача на хранение) – особый метод публикации научных работ (отдельных статей, обзоров, монографий, сборников научных трудов, материалов научных конференций, симпозиумов, съездов, семинаров), разрешенных в установленном порядке к открытому опубликованию.

Подготовка и передача на депонирование научных работ происходит в соответствии с «Инструкцией о порядке депонирования научных работ по естественным, техническим, социальным и гуманитарным наукам» (М., 2014).

Депонированные научные работы находятся на хранении в депозитарии ВИНИТИ РАН, копии работ предоставляются заинтересованным организациям и специалистам на бумажном и электронном носителях и являются официальной публикацией.

Информация о депонированных научных работах включается в информационные издания ВИНИТИ РАН: Реферативный журнал, Базу данных и Аннотированный библиографический указатель «Депонированные научные работы».

Направить научную работу на депонирование можно, обратившись в Группу депонирования ЦНИО ВИНИТИ РАН по адресу:

125190, Москва, ул. Усиевича, 20.
ВИНИТИ РАН, Группа депонирования ЦНИО
Тел.: 499-155-43-28, 499-155-43-76, 499-155-42-43, Факс: 499-943-00-60,
E-mail: cnio@viniti.ru, dep@viniti.ru

С инструкцией о порядке депонирования можно ознакомиться на сайте ВИНИТИ РАН: **http://www.viniti.ru**

ВНИМАНИЮ ПОДПИСЧИКОВ!

С 2018 года возобновляется издание информационного бюллетеня «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления» серии «Экономический и научно-технический потенциал» (56741) взамен информационного бюллетеня «Экономика и управление»

Периодичность выхода – 12 номеров в год. Объем 48 уч.-изд. л. в год.

В бюллетене освещаются материалы иностранной печати по широкому спектру вопросов, касающихся сфер экономического и научно-технического развития России и стран СНГ: общие вопросы, финансы, промышленность, рынки, сельское хозяйство, космос, транспорт и связь, природные ресурсы, трудовые ресурсы, внешние торгово-экономические и научные связи

Оформить подписку на информационный бюллетень, начиная с любого номера, можно в ВИНИТИ РАН по адресу: 125190, Россия, Москва, ул. Усиевича, 20,

Телефоны: (499) 151-78-61; (499) 155-42-85

Факс: (499) 943-00-60;

E-mail: contact@viniti.ru; sales@viniti.ru

ВНИМАНИЮ ЧИТАТЕЛЕЙ!

ВИНИТИ РАН, как единственный в России владелец лицензии Консорциума УДК, предлагает издания УДК полного четвертого издания на русском языке в печатном и электронном виде:

1. Таблицы УДК

УДК. Том I Общая методика применения УДК. Вспомогательные таблицы. Основные таблицы. Общий отдел. Алфавитно-предметный указатель к Общему отделу

УДК. Том II **1/3** Философия. Психология. Религия. Богословие. Общественные науки (только электронное издание)

УДК. Том III **5/54** Математика. Естественные науки (только электронное издание)

УДК. Том IV **55/59** Геологические и биологические науки (только электронное издание)

УДК. Том V **6/61** Медицинские науки (только электронное издание)

УДК. Том VI (часть 1) 6/621 Прикладные науки. Технология. Инженерное дело (только электронное издание)

УДК. Том VI (часть 2) 622/629 Техника. Инженерное дело (только электронное издание)

УДК. Алфавитно-предметный указатель к т. VI (1 и 2 части) (только электронное издание)

УДК. Том VII **63/65** Сельское хозяйство. Домоводство. Управление предприятием (только электронное издание)

УДК. Том VIII **66** Химическая технология. Химическая промышленность. Пищевая промышленность. Металлургия. Родственные отрасли (только электронное издание)

УДК. Том IX **67/69** Различные отрасли промышленности и ремесел. Строительство (только электронное издание)

УДК. Том X **7/9** Искусство. Спорт. Филология. География. История.

УДК. АПУ (с в о д н ы й) к полному 4-му изданию

УДК. Изменения и дополнения. Выпуск 2 (к т.т. 1–3) (только электронное издание)

УДК. Изменения и дополнения. Выпуск 3 (к т.т. 1–6) (только электронное издание)

УДК. Изменения и дополнения. Выпуск 4 (к т.т. 1–7) (только электронное издание)

УДК. Изменения и дополнения. Выпуск 5 (к т.т. 1–10)

УДК. Изменения и дополнения. Выпуск 6 (к т.т. 1–10)

УДК. Изменения и дополнения. Выпуск 7 (к т.т. 1–10), 2017 г. (только электронное издание)

Для подписки необходимо направить заявку по адресу:

125190, Россия, Москва, ул. Усиевича, 20, ВИНИТИ РАН

Телефоны: 499-155-42-85, 499-151-78-61

E-mail: feo@viniti.ru