СПРАВОЧНО-ИНФОРМАЦИОННЫЙ РАЗДЕЛ

УДК [002:351.75] – 049.5

В.В. Арутюнов

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

Рассматриваются итоги состоявшейся в Москве в Российском государственном гуманитарном университете (РГГУ) конференции, на которой было представлено около 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*

DOI: 10.36535/0548-0019-2020-07-5

В апреле 2020 г. в Российском государственном гуманитарном университете (РГГУ) состоялась III Международная научно-практическая конференция «Информационная безопасность: вчера сегодня, завтра», в которой приняли участие около 100 учёных и специалистов. На конференцию, проводившуюся в режиме онлайн, было представлено около 40 докладов; на ней функционировали три секции: Общие вопросы обеспечения информационной безопасности, Программно-аппаратные методы и средства защиты информации, Практика и перспективы развития направлений информационной безопасности.

Основная цель прошедшей конференции – обеспечение эффективного взаимодействия разработчиков и потребителей различной продукции в сфере информационной безопасности с целью ускорения продвижения современных технологий на рынке систем и средств безопасности, а также широкого обмена 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. При этом следует отметить, что для конференции этого года были характерны две особенности: во-первых, в большинстве случаев (около70 %) у докладов было двое и более авторов, что свидетельствует о том, что время исследователей-одиночек, очевидно, уходит в прошлое, и, во-вторых, авторами примерно 30% докладов были представители различных организаций.

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) **"Процессная модель мониторинга и реагирования на инциденты информационной безопасности"** рассматриваются проблемы обеспечения информационной безопасности автоматизированных информационных систем в условиях распределённой сетевой архитектуры их построения. Авторы считают одной из основных задач обеспечения информационной безопасности создание и эффективную реализацию интегрированной системы мониторинга и реагирования на инциденты информационной безопасности. В качестве метода решения этой задачи обосновывается необходимость создания процессной модели мониторинга и реагирования на инциденты информационной

безопасности; предлагается вариант построения этой модели, включающей информационно-технологическую инфраструктуру системы, имеющей выходы для пополнения базы знаний и передачи показателей ситуаций инцидентов лицу, принимающему решения.

Доклад д.т.н. В.В. Арутюнова, к.т.н. Н.В. Гришиной (РГГУ) **"Публикационная активность по результатам исследований в области основных естественнонаучных отраслей знаний как индикатор безопасности государства"** посвящён рассмотрению пяти современных проблем, стоящих перед человечеством в XXI в.: цифровизация, экология, генетика, космос, мировой океан, решение которых немыслимо без развития научно-технического прогресса и обеспечения безопасности государств планеты. Анализ отражаемой в базе данных РИНЦ (Российского индекса научного цитирования) публикационной активности в 2013-2018 гг. российских ученых в области основных естественнонаучных отраслей знаний, определяющих развитие научно-технического прогресса (химии, физики, математики, автоматики и вычислительной техники, информатики), с аналогичными показателями в области информационной безопасности показал практическое совпадение нормализованных показателей публикационной активности для информационной безопасности и указанных групп отраслей за последние четыре года. Этот факт свидетельствует об определённой взаимосвязи этих показателей, когда в различные годы их значения имеют одновременный практически синхронный рост или падение.

В докладе к.т.н. А.С. Мосолова (Российский химико-технологический университет им. Д.И. Менделеева – РХТУ), д.ф.-м.н. Ю.В. Пруса (Российский государственный университет нефти и газа (Национальный исследовательский университет) им. И.М. Губкина), А.Н. Шушпанова (РХТУ) **"Пять шагов к информационной безопасности предприятия"** предлагается концепция формирования системы обеспечения информационной безопасности предприятия. Авторы представляют последовательность проведения необходимых организационных мероприятий, построения процедур, а также осуществления процессов защиты информации в ходе операционной деятельности предприятия.

Первый этап этой концепции (инвентаризация активов компании) включает пять пунктов: от разработки соответствующих форм представления различной информации до описания разнообразных форм хранения информации. Второй этап (техноминимализм) также включает пять пунктов: от правил ведения архивных данных до сохранения и уничтожения соответствующей информации. Наиболее ёмкий третий этап (непосредственная деятельность компании) включает 10 пунктов: от обеспечения физической безопасности до обучения пользователей и документирования соответствующих процедур. Два последних этапа содержат правила утилизации защищаемых активов и персональную ответственность за инциденты в области информационной безопасности.

Концепция была апробирована на примере двух транснациональных компаний – в одной из них схема встраивалась в уже созданный процесс, корректируя опыт ведения защиты активов информационно-технического отдела предшественниками, во втором случае (новая компания) процессы выстраивались с нуля. В обоих случаях схема реализации показала более чем приемлемые результаты.

Доклад д.т.н. В.Г. Бурлова (Санкт-Петербургский политехнический университет Петра Великого), М.И. Грачёва (Санкт-Петербургский университет МВД России) **"Модель управленческого решения как перспективное направление в обеспечении информационной безопасности"** посвящён рассмотрению построения математической модели обеспечения информационной безопасности (ИБ) с учётом человеческого фактора и используемого аппаратно-программного комплекса. Авторы отмечают, что при формировании этой модели должны быть учтены следующие основные допущения:

- факты выявления проблем ИБ имеют случайные проявления во времени, и эти факты образуют поток, близкий к потоку Пуассона;
- затраченное на анализ полученных данных время является величиной случайной;
- при построении модели рассматривается вариант, в котором временной интервал, затраченный на определение проблемы ИБ, равен или меньше суммы временных интервалов, затраченных на определение и устранение проблемы;
- разрабатываемая модель предназначена для оценки показателя эффективности реализации управленческих решений по управлению ИБ.

Авторами получено уравнение вероятности того факта, что проблема ИБ будет найдена и устранена соответствующим управленцем с использованием необходимых ресурсов системы управления.

В докладе д.т.н. И.Д. Королёва, В.И. Попова, Д.И. Ревы (Краснодарское высшее военное училище) **"Обзор методов прогнозирования целенаправленных угроз информационной безопасности"** анализируются актуальные угрозы информационной безопасности, показано место понятия информационной безопасности с точки зрения реализации прогнозирования информационных угроз. Авторами проведена классификация инцидентов информационной безопасности, методов и способов прогнозирования угроз, рассмотрены их достоинства и недостатки.

По результатам анализа методов прогнозирования с учётом появления большого числа новых распределённых во времени методов и способов проведения компьютерных атак, а также несмотря на достоинства каждого из более десятка методов прогнозирования можно выделить следующие их недостатки:

- узкая применимость моделей;
- отсутствие единообразия анализа и проектирования;
- недостаточная гибкость;
- недостоверность прогноза при низкой статистической совокупности исходных данных.

Авторами установлено, что наиболее оптимальным методом выявления инцидентов ИБ может стать метод прогнозирования поведения системы.

В докладе д.т.н. В.А. Минаева, А.В. Симонова (Московский государственный технический университет им. Н.Э. Баумана), **"Выявление контента террористического и экстремистского характера в информационных системах с помощью *DLP*-технологий"** приводятся результаты исследования по анализу текстов экстремистского и террористического характера с помощью применения специального корпусного менеджера; получен реестр наиболее часто встречаемых слов и словосочетаний, содержащихся в контекстах такого рода. Предложенный авторами подход открывает перспективные направления для использования *DLP*-систем, в которых применяются технологии предотвращения утечек конфиденциальной информации из информационной системы, в более широком контексте – для выявления распространения экстремистского контента. А именно, на основе специально созданных корпусов текстов возможно выявление экстремизма в широком смысле: антисемитизм, русский радикальный национализм, христианский шовинизм, а также сектантские движения, запрещённые в России (саентологическое движение, деятельность свидетелей Иеговы и т д.).

По мнению авторов дальнейшие перспективы обеспечения информационной безопасности в плане защиты пользователей, в том числе социальных сетей, от негативных информационных воздействий путём специальной обработки, анализа и оценки их контента связаны с использованием методов глубокого машинного обучения и искусственного интеллекта для решения задач обеспечения информационной безопасности, эффективность применения которых несомненно выше традиционных статистических методов автоматической обработки текста, что подтверждают результаты данной работы.

В докладе Д.В. Чемарева (Дальневосточный юридический институт МВД России) **"Апробация системно-динамической модели анализа и оценки системы защиты информации от внутреннего нарушителя при помощи платформы имитационного моделирования *ANYLOGIC*"** представлены результаты апробации разработанной системно-динамической имитационной модели анализа и оценки системы защиты информации от внутреннего нарушителя при помощи платформы имитационного моделирования Anylogic.

Апробация модели проводилась для своего рода граничных значений, а именно – для крайне лояльного сотрудника и крайне нелояльного. Такой подход позволяет сравнивать итоговые результаты со статистическими данными и, таким образом, подтверждать адекватность разработанных моделей, а также наглядно оценивать эффективность системы защиты при различных её настройках. В ходе экспериментов выяснилось, что при оптимальных настройках системы защиты модель оказывает неоценимую помощь при расследовании инцидентов, сокращая время на установление всех фактов и формируя доказательную базу. Кроме того, в случае необходимости и при наличии определённых ресурсов, система защиты может быть настроена таким образом, что реализация кражи информации будет практически невозможна. Апробация данной модели показала также эффективность борьбы с инсайдером как на стадии планирования реализации угрозы, так и на стадии разбора инцидента.

В докладе д.т.н. С.И. Неизвестного (Финансовый университет при Правительстве РФ) **"Распределение ресурсов предприятий в управлении инцидентами информационной безопасности и информационными рисками"** отмечается, что подавляющее большинство компаний российского ИТ-бизнеса в управлении ИБ значительные ресурсы выделяет на управление инцидентами в ущерб ресурсам на управление информационными рисками (упреждения инцидентов).

Западные компании, находящиеся на 4-м и 5-м уровнях зрелости ИТ-бизнеса, согласно системе оценки CMMI / IPMA, большую часть ресурсов ИБ направляют на управление информационными рисками по сравнению с объёмов ресурсов, предназначенных для работы непосредственно с инцидентами. Положение с этой проблемой в российском бизнесе можно объяснить, прежде всего, тем, что в России нет организаций с уровнем зрелости ИТ-бизнеса, равным трём и выше, что следует из данных по соотношению уровня зрелости ИТ-бизнеса и элементов управления рисками и инцидентами ИБ, приводимых автором.

Таким образом, на предприятиях высокого уровня зрелости ИТ-бизнеса, по мнению автора, основной значительный объем ресурсов управления информационной безопасностью должен выделяться именно для управления рисками ИБ и лишь небольшая часть ресурсов – для управления инцидентами ИБ.

В докладе к.т.н. В.В. Храмова, А.А. Горбачёвой (Южный университет "Институт управления бизнеса и права"**),** Д.П. Фомичёва (Российский технологический университет (МИРЭА)) **"Моделирование недекларированной активности программного средства в условиях нечеткости исходных данных"** исследуются вопросы формирования нечеткой модели критического свойства программного средства – агрессивности, характеризуемой возможностями по нелегитимному перехвату управления у операционных систем в процессе выполнения программ, находящихся в памяти компьютера. Этот показатель агрессивности определяется уровнем "заражённости", характеризующим мощность конечного множества агрессивных программных элементов в программном средстве, и уровнем опасности и саморепродукции, характеризующим способность программного средства к производству других программных средств.

Для «агрессивного» программного средства, имеющего нерезидентный механизм распространения в вычислительной среде, процесс саморепродукции описывается дискретным марковским процессом. Решение системы дифференциальных уравнений даёт ряд распределения числа нерезидентных программных закладок на конкретный момент времени.

По мнению авторов, рассмотренное новое свойство программного средства позволяет прогнозировать его влияние на ход вычислительного процесса.

В докладе к.т.н. П.Ю. Филяка, А.А. Изъюрова, И.А. Тырина, Д.А. Пажинцева (Сыктывкарский государственный университет) **"Обеспечение информационной безопасности киберфизических систем (*CPS*)"** отмечается, что под киберфизическими системами (*Cyber-Physical Systems – CPS*) понимаются системы, которые состоят из различных объектов и подсистем: объектов природного характера, подсистем искусственного происхождения, а также устройств управления. Во многих случаях киберфизические системы обеспечивают оперативный контроль над фактическими процессами и устройствами, позволяя физическим устройствам анализировать окружающую среду и осуществлять с ней оперативное взаимодействие.

Авторы рассматривают *CPS* как пятикомпонентную систему, включающую следующие элементы: персонал, точка входа в систему, вычислительный блок и обеспечивающие его функционирование подсистемы, датчики состояния технологических процессов и оборудования, исполнительные элементы.

Для каждого элемента системы выполнена классификация соответствующих уязвимостей и угроз информационной безопасности.

* * *

По итогам прошедшей в РГГУ конференции издан сборник трудов её участников[1].

Материал поступил в редакцию 26.04.20.

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: сборник статей III Международной научно-практической конференции / под ред. В.В. Арутюнова. – М.: РГГУ, 2020. – 194 с.

ВНИМАНИЮ ЧИТАТЕЛЕЙ!

ИЗДАНИЕ УДК

УНИВЕРСАЛЬНАЯ ДЕСЯТИЧНАЯ КЛАССИФИКАЦИЯ

АЛФАВИТНО-ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

в 2-х томах

Алфавитно-предметный указатель (АПУ) к 4-му полному изданию УДК на русском языке:

Том I содержит АПУ от буквы А до Н;

Том II содержит АПУ от буквы М до Я и указатель латинских наименований к классам УДК 56 Палеонтология, 57 Биологические науки, 58 Ботаника, 49 Зоология, 61 Медицинские науки.

АПУ содержит около 100 000 понятий, представленных в полных таблицах УДК.

При его составлении были учтены изменения, опубликованные в Выпусках № 1 – 6 «Изменения и дополнения к УДК»

Для подписки необходимо направить заявку для оформления счета по адресу:

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

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

E-mail: feo@viniti.ru

http://www.udcc.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

УВАЖАЕМЫЕ КОЛЛЕГИ!

ВИНИТИ РАН предлагает Вашему вниманию Реферативный Журнал в электронной форме

РЖ в электронной форме (ЭлРЖ) выпускается по всем разделам естественных, технических и точных наук.

Каждый номер ЭлРЖ является полным аналогом печатного номера РЖ по составу описаний документов, их оформлению и расположению. Он сопровождается оглавлением, указателями.

ЭлРЖ представляет собой информационную систему, снабженную поисковым аппаратом и позволяющую пользователю на персональном компьютере:

- читать номер РЖ, последовательно листая рефераты;
- просматривать рефераты отдельных разделов по оглавлению;
- обращаться к рефератам по указателям авторов, источников, ключевых слов;
- проводить поиск документов по словам и словосочетаниям;
- выводить текст описаний документов во внешний файл.

ЭлРЖ в версии Windows Вы можете получить за текущий год с любого номера, а также за предыдущие годы.

Подробную информацию Вы можете получить:

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

Телефон 499-155-42-85 499-151-78-61

E-mail: Contact@viniti.ru, Feo@viniti.ru