СПРАВОЧНО-ИНФОРМАЦИОННЫЙ РАЗДЕЛ

УДК 005.745(100):[002:004.056]

В.В. Арутюнов

Об итогах IV Международной научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра»

Рассматриваются итоги состоявшейся в Москве в Российском государственном гуманитарном университете (РГГУ) конференции, на которую 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, аппаратные средства защиты, информационные системы, программные средства защиты, система защиты информации.*

DOI: 10.36535/0548-0019-2021-07-5

В Российском государственном гуманитарном университете (РГГУ) в апреле 2021 г. состоялась IV Международная научно-практическая конференция «Информационная безопасность: вчера сегодня, завтра», в которой приняли участие более 70 учёных и специалистов. На конференцию, проводившуюся в режиме онлайн в условиях продолжающейся пандемии коронавирусной инфекции, 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 между разработчиками и потребителями различной продукции в сфере информационной безопасности (ИБ) 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 глубине и широте обсуждавшихся проблем в определённой мере свидетельствуют не только названия секций конференции, но и тематика докладов. При этом следует отметить, что для конференции этого года было характерно активное участие аспирантов и студентов старших курсов вузов. Их количество составило около 15% от числа всех участников конференции.

Далее приводится 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) **"Обнаружение вторжений и реагирование на атаки в информационно-технологическом пространстве объектов информатизации"** предлагается решение системной задачи обеспечения ИБ в информационно-технологическом пространстве при сетевой информационно-технологической инфраструктуре организации. Решение базируется на применении риск-ориентированного подхода и процессных методов его реализации. Рассмотрены подходы к процессному моделированию мониторинга состояния и реагированию на атаки. Предложена структура обеспечения ИБ, включающая следующие уровни: менеджмента, аналитических решений и прогноза; корпоративной инте грации; информационно-технологической интеграции; инструментально-технологический. Такая структура существенно повышает эффективность обеспечения ИБ и может быть использована в качестве исходной осно-

вы при создании политики информационной безопасности организации в разделе менеджмента ИБ.

Доклад д.т.н. В.В. Арутюнова (РГГУ) **"Особенности динамики формирования цифрового кластера знаний о результативности и востребованности итогов исследований российских учёных в области форензики"** посвящён рассмотрению динамики изменения в 2010-2019 гг. наукометрических показателей (публикационной активности, цитируемости и индекса Хирша) в области форензики - отрасли знаний, связанной с расследованием преступлений, совершённых с компьютерной информацией, методами получения и исследования доказательств, которые связаны с ней, а также о применяемых для этого программных и технических средствах. Отмечается, что уровень научной активности российских учёных в данной сфере исследований, определяемый с учётом индекса Хирша, превышает минимальное значение национального уровня научной активности российского учёного.

Выявлены особенности изменения вышеуказанных показателей, а также основные направления работ в анализируемой области знаний, итоги которых отличаются высокой востребованностью. В их числе: использование криминалистического компьютерного моделирования при планировании расследования преступлений, особенности следообразования при совершении преступлений с использованием сети Интернет, проблемы назначения компьютерно-технической экспертизы мобильных телефонов при расследовании преступлений, электронные следы в системе криминалистики, преодоление противодействия расследованию преступлений в сфере компьютерной информации.

В докладе М.Ю. Пруса (Российская академия народного хозяйства и государственной службы при Президенте РФ), А.А. Кондратюка (Российский государственный университет нефти и газа (НИУ) им. И.М. Губкина), д.ф.-м.н. Ю.В. Пруса (Российский государственный университет нефти и газа (НИУ) им. И.М. Губкина), к.т.н. В.С. Путина (Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России) **"Стохастическое моделирование каскадных аварий на потенциально опасных объектах"** предлагается каскадная стохастическая модель, описывающая динамику возникновения и развития аварийных и критических состояний в системе, инициируемых локальными инцидентами. Предлагаемая дискретная модель системы основана на представлении набора возможных элементарных состояний в виде стратифицированного графа, что позволяет выделять возможные сценарии развития последовательности событий при возникновении различных инцидентов. Применение трёхпараметрического распределения Вейбулла адекватно и точно описывает динамику интенсивностей переходов между элементарными состояниями. Полученные для избранного сценария при различных инцидентах локальные решения систем уравнений Колмогорова-Чепмена позволяют проводить численное моделирование и анализ динамики рисков возникновения и развития аварийных и критических состояний и определяют «окно возможностей» торможения процессов развития событий по неблагоприятному сценарию и дальнейшего снижения степени опасности вплоть до устранения угроз и ликвидации негативных последствий инцидента при своевременном реагировании служб безопасности, оперативных, аварийно-спасательных и иных подразделений экстренных служб.

В докладе к. ист. наук Г.А. Шевцовой, С.А. Батищева (РГГУ) **"Информационное пространство Российской Федерации как безопасная информационная среда"** исследуется информационное пространство России как информационной среды, безопасной для её населения. Актуальность исследования обусловливается тем, что информационное пространство страны становится одной из площадок глобального информационного противоборства на фоне развивающегося недоверия к традиционным средствам массовой информации, а также к информации как таковой; акцентируется внимание на том, что для населения России весьма чувствительны практически любые виды мошенничества в сети Интернет, связанные с их персональными данными. Авторы фокусируют внимание на том, что существующее в настоящее время несовершенство современного информационного пространства препятствует его полноценному функционированию в интересах государства и общества.
В информационном пространстве продуцируется ограниченная виртуальная реальность, которая не расширяет, а наоборот, в определённой мере сужает возможности человека; отмечается необходимость целенаправленных действий по формированию информационной среды, безопасной для населения России.

Доклад М.И. Грачёва (Санкт-Петербургский университет МВД России), д.т.н. В.Г. Бурлова (Санкт-Петербургский политехнический университет Петра Великого) **"Модель решения информационной безопасности WEB-сайта образовательной организации"** посвящён рассмотрению вопросов управления web-ресурсами организации на основе модели управленческого решения, включающей программные и аппаратные ресурсы, а также человеческий фактор. В докладе приводится уравнение вероятности того, что проблема будет выявлена и устранена лицом, принимающим решение, с использованием или не использованием необходимых ресурсов системы управления. Соотношение было выведено методом решения системы линейных алгебраических уравнений с помощью дифференциальных уравнений А.Н. Колмогорова.

В докладе д.т.н. В.А. Минаева (Московский технический университет МВД России им. В.Я. Кикотя), А.В. Симонова (Московский государственный технический университет им. Н.Э. Баумана), А.Д. Ребровой (Московский государственный технический университет им. Н.Э. Баумана) **"Автоматизированное выявление деструктивного контента в социальных медиа"** обсуждаются модели классификации текстового контента и методы его предварительной

обработки с целью выявления деструктивных воздействий в социальных медиа. Под деструктивным контентом авторы понимали информационный контент в социальных медиа с призывами к разжиганию национальной и религиозной розни, распространение через Интернет информации о наркотических и иных губительных для человека, особенно – молодежи, веществах, материалов, содержащих порнографию, в том числе – с участием несовершеннолетних, а также пропаганду террористических, экстремистских и иных криминальных действий.

Исследованы и применены основные методы векторизации текстов: Bag of Words, TF_IDF, Word2vec. Авторами выявлено, что наиболее высокую точность (0,97) при решении задачи распознавания деструктивного контента даёт системная интеграция алгоритма векторизации Bag of Words, метода главных компонентов для снижения пространства признаков описания текстов, а также логистической регрессии как моделей обучения.

Доклад д.т.н. Е.Н. Надеждина **"Алгоритм обнаружения сетевых атак на основе идентификации динамических характеристик сетевого трафика"** (РГГУ) посвящён проблеме раннего выявления сетевых атак на компоненты корпоративной информационной сети на основе сбора и анализа данных о состоянии сетевого трафика. Автором аргументирована концепция инновационного программно-аппаратного комплекса обнаружения сетевых атак, а также теоретически обоснован и экспериментально апробирован новый способ обнаружения распределённых атак "отказ в обслуживании" (DDoS-атак) и их комбинаций, использующий выделение и последующую обработку вторичных показателей, характеризующих динамическую структуру сетевого трафика.

По итогам исследовательской деятельности создан программно-аппаратный комплекс, отличительной особенностью которого является способность обнаруживать отклонения в трафике с априорно заданными вероятностями обнаружения. Данный эффект достигается за счёт применения комбинированного подхода, основанного на методе последовательного анализа Вальда и авторских методиках преобразования и интеллектуального анализа информационных признаков агрегатов пакетов данных.

В докладе д.т.н. С.В. Вепрева, к.т.н. С.А. Нестеровича **"Меры по совершенствованию защищённости персональных данных в сети интернет"** (Московская академия Следственного комитета Российской Федерации) рассматриваются уязвимости персональных данных, определены основные нормативно-правовые акты, регламентирующие правоотношения в сфере персональных данных. Показаны наиболее часто встречающиеся случаи нарушения Федерального закона РФ от 27.07.2006, № 152-ФЗ «О персональных данных», а также предложены некоторые мероприятия по защите персональных данных.

Авторы считают необходимым на официальном уровне обеспечить бесплатное оформление электронной цифровой подписи для каждого гражданина страны, достигшего совершеннолетнего возраста. Данная мера будет способствовать обеспечению безопасности персональных данных, в том числе их целостности; электронная подпись также будет идентифицировать пользователя, отправляющего документы в государственные органы. При этом требуется на законодательном уровне установить максимальный срок хранения персональных данных, регламентировать процедуру уничтожения этих данных и ввести соответствующие административные наказания за нарушение ограничений и требований вышеуказанного закона.

В докладе С.В. Городилова (Группа технических компаний “АСПЕКТ СПб”, г. Киров), И.К. Сухих (Вятский государственный университет), д.т.н. А.В. Частикова (Вятский государственный университет) **"Увязывание концепции менеджмента и нормативно-правовых требований информационной безопасности в модели управления организацией"** показаны проблемы, с которыми сталкиваются организации при необходимости увязывания в одной управленческой модели двух различающихся подходов к управлению ИБ. С одной стороны, необходимо применять различающееся нормативное регулирование РФ, как правило, устанавливающее требования ИБ в контексте жизненного цикла информационных систем. С другой стороны, известные международные концепции управления ИБ, такие как, например, ISO 27001, подходят к объектам защиты и мерам ИБ в контексте риск-ориентированного подхода и необходимости постоянного совершенствования ИБ. Предложен подход, который позволяет путем применения нотации IDEF0 объединить указанные направления в одной модели управления организацией.

Модель процессов управления ИБ организации, описанная авторами с помощью стандарта IDEF0, позволяет решить проблему увязывания в одной управленческой модели нормативного регулирования, основанного на жизненных циклах защищаемых объектов, и менеджмента ИБ. При этом применение декомпозиции и итеративного подхода при создании модели приводит к системному представлению о всех процессах организации в сфере ИБ.

В докладе д.т.н. И.Д. Королёва, Д.И. Маркина (Краснодарское высшее военное училище) **"Сравнительный анализ средств эмуляции автоматизированных систем"** определена необходимость эмуляции автоматизированных систем (АС) при тестировании на проникновение в рамках контроля защищённости. Исследованы симуляторы дискретных событий, эмуляторы распределённой вычислительной сети, виртуальные среды для тестирования; выявлены наиболее подходящие для выполнения поставленных задач средства эмуляции.

По результатам проведенного анализа авторами сделан вывод, что наиболее эффективно решить поставленную задачу по созданию модели функционирования АС возможно при использовании симуляторов распределённых вычислительных сетей. Имитацию функционирования АС при этом целесообразно

осуществлять с использованием специальных программ-ботов, запускаемых на конкретных узлах сформированной модели. Применение средств симуляции дискретных событий для эмуляции АС, по мнению авторов доклада, представляется нецелесообразным из-за высокого уровня абстракции подобных систем. При этом сама процедура описания узлов распределённой вычислительной сети и действий пользователей и нарушителей ИБ требует высокого уровня навыков работы с конкретным симулятором и значительного количества временных ресурсов.

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

Материал поступил в редакцию 25.04.21.

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 IV Международной научно-практической конференции / под редакцией В.В. Арутюнова. – Москва : РГГУ, 2021. – 198 с.