ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В СОЦИАЛЬНЫХ СЕТЯХ: МОДЕЛИ И МЕТОДЫ ИССЛЕДОВАНИЯ

В.А. Минаев

В статье показано, что значимым научно-практическим ресурсом достижения требуемого уровня противоборства в социальных сетях (СС) является обращение к современным методам моделирования с применением передовых информационных технологий. Исследуются актуальные вопросы теоретического, методического и прикладного обеспечения, направленного на выработку практических рекомендаций по управлению информационным противодействием в СС и определения перспективных направлений разработки моделей в указанной сфере. Показано, что существующие модели и методы не позволяют в полной мере исследовать факторы, определяющие особенности распространения деструктивной информации в СС, учесть некоторые латентные факторы в этой сфере. Имеющимся моделям характерна слабая возможность имитации различных динамических ситуаций, что накладывает определенные ограничения на обоснованность решений в сфере противодействия деструктивной информации. Детально рассмотрены особенности ее распространения в СС, включая деструктивное воздействие со стороны террористических и экстремистских структур. Даны основные понятия из сферы информационного противоборства. Охарактеризованы деструктивные информационные воздействия на современное общество, угрозы информационно-психологической безопасности пользователям СС и меры противодействия указанным угрозам. Освещены опыт и методологические вопросы моделирования информационного противоборства в СС. Особое внимание акцентировано на системно-динамический и агентный подходы, реализованные в виде имитационных моделей. Сделан вывод, что системно-динамический подход позволяет наиболее качественно описывать распространение негативных информационных воздействий и процессы противоборства в СС.

Ключевые слова: информационная безопасность, информационное противоборство, системно-динамическая модель, деструктивная информация, социальная сеть.

ФОРМАЛИЗАЦИЯ ОПИСАНИЯ МОНОВИРУСНЫХ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ В СЕТЯХ

А.Г. Остапенко, Е.С. Соколова, Ю.Г. Пастернак, Е.А. Шварцкопф, К.В. Сибирко, В.В. Сафронова

Рассматривается процесс распространения вирусной инфекции (компьютерной, психологической) в сетевой структуре в корпоративной, социальной сети. Предлагается обобщенная модель вирусования элемента сети с учетом дискретности его состояний (статусы восприимчивого к вирусу элемента, распространителя инфекции, иммунизированного элемента). Шаг моделирования (дискретного) сопоставим с инкубационным периодом. В этой связи рассматривается риск появления (в эпидемическом процессе) множества элементов сети различных (из вышеупомянутых) статусов на основе веерного представления процесса. По их количественной оценке прогнозируется эпистойкость сети в отношении рассматриваемого вируса.

Ключевые слова: вирус, эпидемия, моделирование, сеть, риск.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В БЕСПРОВОДНЫХ ИК-КАНАЛАХ ПЕРЕДАЧИ ДАННЫХ

А.В. Бабурин, Л.А. Глущенко, Б.Н. Добряков

Цель исследования состоит в разработке методов защиты от несанкционированного доступа информации, циркулирующей в беспроводных ИК-каналах передачи данных. Показаны возможные способы несанкционированного доступа к каналу передачи данных от ИК-клавиатуры к компьютеру. Основной способ несанкционированного доступа к ИК-каналу передачи данных – это регистрация диффузно-отраженного от элементов интерьера излучения. Проведены теоретические оценки, подтверждающие возможность получения информации, циркулирующей в беспроводных ИК-каналах передачи данных при несанкционированном доступе. Рассмотрен типичный случай распространения излучения в помещении при использовании ИК-канала передачи данных при несанкционированном доступе. Неуполномоченный наблюдатель может регистрировать через оконный проем диффузно-отраженное излучение, используя специальную оптико-электронную систему. Для расчетов были приняты типовые фотометрические характеристики интерьера помещения и предельно достижимые на современном уровне техники характеристики фотоприемных устройств. Размер диаметра входного зрачка оптической системы принят не слишком большим из того соображения, что он не должен привлекать внимание (служить демаскирующим признаком). Предложен метод защиты информации, циркулирующей в беспроводных ИК-каналах передачи данных, основанный на формировании засветочных помех. Приведены схемы формирования засветочных помех. Для помехи может быть использовано диффузно-отраженной излучение или специально сформированное излучение, направленное на оконный проем помещения.

Ключевые слова: светоизлучающий диод, беспроводные ИК-каналы передачи данных, несанкционированный доступ, засветочные помехи.

К ВОПРОСУ О ТРЕНДАХ И ИНСТРУМЕНТАРИИ СОЦИО-ИНФОРМАЦИОННОГО ГЛОБАЛЬНОГО ПРОТИВОБОРСТВА

А.Г. Остапенко, А.А. Остапенко, Н.М. Лантюхов, С.Д. Трубицын, И.А. Боков

Вниманию читателя предлагается краткий обзор интернет-прогнозов и сценариев глобального развития, спровоцированных пандемией коронавируса: цифровой контроль, перезагрузка парадигмы, эпидемия агрессии, вспышка региональных конфликтов, деградация западного либерализма, беспрецедентная информационная война. В контексте перечисленных инфодемических тенденций рассматривается инструментарий противоборства в социо-информационном пространстве, включая способы «замедления трафика» и «гиперболизации очернения», а также – приемы «отвлекающего вброса» и «шарманки». Предпочтение отдается информационно-психологическим интернет-дуэлям, в отличии от средств блокирования противника, применение которых авторы не считают эффективными в долгосрочной перспективе сетевого противодействия.

Ключевые слова: социо-информационное пространство, пандемия коронавируса, способы и приемы информационного противоборства, тренды, турбулентность.

3D-ПРИНТЕРЫ – РЕАЛЬНОСТЬ И БУДУЩЕЕ. АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, Д.А. Пажинцев, И.А. Тырин

На сегодняшний день на современном уровне развития технического прогресса человечество разработало множество устройств и способов создания трехмерных тел (объемных тел), каждый из которых имеет как свои преимущества, так и недостатки. Среди этого перечня особого внимания заслуживают устройства, которые имеют целый ряд неоспоримых преимуществ. Во-первых, они позволяют тиражировать трехмерные тела практически в неограниченных количествах. Во-вторых, точность построения объемных фигур очень высока. В-третьих, они позволяют работать с любыми материалами, в зависимости от применения которых, могут получаться различные трехмерные объекты – от реальных строительных объектов – до реальных тканей и органов растительных и живых организмов. Причем объектов, как макроскопических размеров – десятки метров, так и микроскопических, вплоть до нано уровня. Эти устройства вошли в обиход под названием «3D – принтеры». 3D-принтер – это периферийное устройство для создания физического объекта путем послойного формирования его по его цифровой 3D-модели. Данное устройство тесно связано с нашей жизнью. С каждым днем человек находит новое применение для 3D-принтеров, эти устройства уже являются незаменимыми помощниками во многих сферах нашей жизнедеятельности. Создание 3D-принтера, несомненно, является технологическим прорывом.

Ключевые слова: SLA - печать, SLS – печать, FDM – печать, информация, трехмерная цифровая модель изображения, рабочий стол, экструдер, слайсинг, 3-D принтер, интернет вещей, уязвимость, информационная безопасность.

«ИНФОДЕМИЯ» И СОЦИАЛЬНЫЕ СЕТИ: АКТУАЛЬНЫЕ ОБЪЕКТЫ И ЗАДАЧИ ИССЛЕДОВАНИЯ

А.Г. Остапенко, Р.В. Сорокин, С.В. Лихобабин, А.О. Ткаченко, А.Н. Бартенев, Ю.Г. Пастернак

В данной статье затрагивается тема мировой инфодемии в контексте информационного влияния и давления на общественность, во многом образованную пользователями Интернет-пространства. В работе ведется рассуждение об актуальности исследования социальных Интернет-сайтов и процессов распространения в них потенциально опасных контентов. Описаны общие характеристики целеполагания исследований в различных областях таких как: суверенизация информационного пространства, анонимности и ответственности интернет-пользователей, контроля трафика, инфодемии, применения систем искусственного интеллекта в Интернет-пространстве.

Ключевые слова: инфодемия, опасный контент, информационная безопасность, риск.

ФОРМАЛИЗАЦИЯ ПОДХОДА К ОПРЕДЕЛЕНИЮ СТЕПЕНИ СОЦИАЛЬНОГО УЩЕРБА ДЛЯ ОПЕРАТОРОВ ИНФОРМАЦИОННЫХ СИСТЕМ

О.М. Голембиовская, Е.В. Кондрашова, М.Ю. Рытов, К.Е. Шинаков

На сегодняшний день в нормативно-правовой базе Российской Федерации отсутствуют точные механизмы определения степени ущерба от нарушения свойств информационной безопасности. Имеющиеся упоминания о степени ущерба (Приказ № 17ФСТЭК, проект методики ФСТЭК 2015 года) предлагают экспертный аппарат определения точных значений степени ущерба, а, следовательно, полученные результаты у экспертов разных направленностей и уровня знаний будут разными. В данной статье приведен подход к определению степени социального ущерба, основанный на проекте методики ФСТЭК по определению угроз безопасности информации в ИС от 2015 года.

Ключевые слова: безопасность, информация, подход, степень, ущерб.

КРАТКИЕ НАУЧНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ФОРМИРОВАНИЮ И ВЫПОЛНЕНИЮ ТЕХНИЧЕСКИХ ЗАДАНИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Г. Остапенко, М.Е. Волкова, Д.А. Нархов, А.А. Остапенко, А.В. Заряев, Т.Ю. Мирошниченко, П.Д. Федоров

В статье описаны основные научно-методические рекомендации для исследовательских работ в области информационной безопасности (ИБ). Озвучена основная терминология, которая применяется для написания творческих работ, и особенности классифицированного дерева, способствующего фундаментальному анализу угроз и рисков. Перечислены (в контексте исследования) пункты, основной мыслью которых является неприемлемость, использования информации, не имеющей под собой достаточно мощную теоретическую и доказательную базу. Прописаны рекомендации по структуре проектных работ в сфере ИБ и приведены примеры формализации базовых элементов творческих работ в области обеспечения ИБ. Обоснована необходимость решения задач, связанных с модернизацией ПТК «Netepidemic».

Ключевые слова: риск, угрозы, исследовательская работа, аналитическая оценка.

ОЦЕНКА РИСКА БЕЗОПАСНОСТИ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ

А.А. Болгов, С.А. Ермаков, Л.В. Паринова, Н.И. Баранников

В статье предлагаются результаты анализа возможности применения традиционных подходов к анализу рисков в сетях Интернета вещей с учетом особенностей архитектуры построения и динамики их развития. До настоящего времени было предложено множество методов для решения таких проблем с использованием вероятностных моделей. Но несмотря на то, что они позволяют решить большинство задач, они все же могут вызывать некоторые проблемы при оценке рисков и анализе полученных результатов. Наиболее распространенные проблемы связаны со сложностью ранжирования и объективностью оценки вероятности нанесения ущерба и величины этого ущерба. По итогу к заключению статьи приводятся аргументы в пользу альтернативных методологий анализа рисков, адекватно учитывающих динамические характеристики технологии при сохранении преимуществ существующих подходов к оценке.

Ключевые слова: технология Интернета вещей, риск-анализ, беспроводные сети, защищенность, эффективность.

РЕАЛИЗАЦИЯ ПРОЕКТА МОДЕРНИЗАЦИИ ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА ЭПИДЕМИЧЕСКОГО РИСК-МОДЕЛИРОВАНИЯ «NETEPIDEMIC»

Е.Р. Нежельский, А.К. Журавлев, В.В. Исламгулова, К.А. Разинкин, И.Л. Батаронов, В.Г. Юрасов

С каждым годом происходит рост атак злоумышленников на информационные системы с применением как вредоносного кода, так и методов социальной инженерии и вредоносных контентов. Существующие системы анализа эпидемических процессов предоставляют в основном средства визуализации результатов моделирования и не подходят для практического применения с целью воспроизведения реальных процессов диффузии вредоносного кода и контента в распределенных автоматизированных информационных системах. В статье приведена последовательность мероприятий, проведенных в рамках модернизации программно-технического комплекса «NetEpidemic» в направлении риск-мониторинга эпидемических процессов, протекающих в информационных системах, отвечающего требованиям в первую очередь прогнозирования и качественной визуализации результатов с целью его актуализации как инструмента научно-исследовательских изысканий и дальнейшего продвижения на рынке программного обеспечения.

Ключевые слова: программно-технический комплекс, распределенные автоматизированные информационные системы, риск-моделирование, эпидемический процесс, макро- и микромоделирование, риск-метрология, визуализация.

ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПОДХОДЫ. ДИСКУРС (ПРЕДЫСТОРИЯ)

П.Ю.Филяк, В.В. Пименова

Настоящая статья посвящена информационной безопасности. Точнее, одной из составляющей понятия информационная безопасность, а если говорить более стандартизованно, то одному из ее аспектов, то есть выражаясь корректно, профессиональным языком (используя профессиональную стандартизованную терминологию) – «Гуманитарным аспектам информационной безопасности» (ГАИБ). Если говорить о ГАИБ, то рассмотрении этого термина необходимо начинать с макро уровня сферы информационной безопасности, то есть на уровне обеспечения информационной безопасности в масштабах государства. Если рассматривать информационную безопасность как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, то в качестве целей и задач ГАИБ должны рассматриваться прежде всего защищенность как отдельной личности (*humanitas* - *гуманитарный*), так и всего социума, который и являет собой в итоге и общество и государство в целом, причем рассматривать ее с разных точек зрения (*аспектов*). Отсюда и происходит обозначенный выше термин – гуманитарные аспекты информационной безопасности (ГАИБ). Таковы исходные императивы при рассмотрении вопросов и проблем, затрагиваемых в рамках настоящей статьи.

Ключевые слова: информация, гуманитарный, аспект, информационная безопасность, гуманитарные аспекты информационной безопасности, информационная война, информационное оружие, информационное воздействие, информационный сигнал, информационно-телекоммуникационные системы, социальные сети, блогер.