КИБЕРПРОСТРАНСТВО КАК ОБЪЕКТ ИССЛЕДОВАНИЯ И ЗАЩИТЫ. ЧАСТЬ 1

А.Л. Сердечный

Работа посвящена описанию киберпространства как защищаемого объекта, обладающего уникальными свойствами по сравнению с другими видами пространств (водным, земным, воздушным и космическим). В рамках проведённых исследований рассмотрены различные определения данного понятия и выделены его основные аспекты. Рассмотрение киберпространства в этих аспектах позволило выявить основные закономерности его генезиса и эволюции о которых также рассказывается в настоящей статье. Также было показано, что сложность и размер киберпространств требует особых подходов его изображения и исследования, в том числе, через анализ субъектов, которые его порождают, а также действуют в нём. Фактически предлагается новый взгляд на специфическое пространство, порожденное человечеством, которое сегодня проникло во все сферы общественной деятельности и остро нуждается в защите и глубоком исследовании (в том числе и картографическими методами).

Ключевые слова: киберпространство, генезис киберпространства, эволюция киберпростарнства, представление киберпростарнства.

КИБЕРПРОСТРАНСТВО КАК ОБЪЕКТ ИССЛЕДОВАНИЯ И ЗАЩИТЫ. ЧАСТЬ 2

А.Л. Сердечный

В статье рассматриваются основные аспекты исследования киберпространства: территория, сетевое представление и расстояние между расположенными в нём объектами. Показана возможность многокомпонентного представления киберпространства в виде системы уровней взаимосвязанных объектов: физического, информационного и социального. Обсуждаются возможности регулирования защищаемого киберпространства со стороны его различных субъектов. Уделяется внимание большим данным, циркулирующим в киберпространстве. Рассматриваются возможные подходы к исследованию защищаемого киберпространства, включая шаблонно-онтологический, теоретико-игровой, сетевой и геопространственный подходы. Приводятся преимущества и ограничения каждого из них. Особое внимание уделяется картографической методологии исследования защищаемого киберпространства, в связи с чем в качестве иллюстрации его основных идей рассматривается информационная карта поиска научных публикаций по теме «Картография защищаемого киберпространства». В заключении формируются задачи разработки реализации картографической методологии исследования защищаемого киберпространства.

Ключевые слова: защищаемое киберпространство, территория киберпространства, большие данные, информационная карта.

ИМИТАЦИЯ ФУНКЦИОНИРОВАНИЯ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РЕАЛИЗАЦИИ КИБЕРАТАК

В.А. Минаев, Е.С. Поликарпов

Статья посвящена проблеме моделирования работы центра информационной безопасности предприятия (ЦИПБ) в условиях реализации кибератак. Имитационная модель позволяет решать широкий спектр задач, в частности, задач управления временем обработки сообщений об инцидентах безопасности, оптимизации ресурсного обеспечения информационной безопасности предприятия, ее прогнозирования. Показано, что для решения указанных хорошо применимы методы дискретно-событийного моделирования. Дискретно-событийная модель ЦИБП отражает современные тренды в области технологического обеспечения информационной безопасности предприятий и организаций; учитывает наиболее существенные факторы, влияющих на характеристики информационной безопасности предприятий; обеспечивает баланс между требуемой точностью результатов моделирования и сложностью модели; отличается универсальностью, адаптивностью для решения многих задач управления информационной безопасностью, гибкостью разработки моделей в современной среде имитационного

моделирования. В качестве среды имитационного моделирования выбрано программное обеспечение отечественного производства Anylogic, позволившее проигрывать различные сценарии кибератак на ЦИБП, помогающее качественно интерпретировать результатов реализации моделей, провести различные виды имитационных экспериментов, в том числе – по вариации параметров моделей, анализу их чувствительности, оптимизации ресурсного обеспечения информационной защиты. Сделан вывод, что дальнейшим развитием исследования ЦИБП предприятий является уточнение и детализация модели, структуры ее блоков и содержания сообщений о компьютерных инцидентах.

Ключевые слова: кибератака, предприятие, информационная безопасность, дискретно-событийное моделирование, SIEM-система, SOC-центр, имитация.

ПРИМЕНЕНИЕ ГЛУБИННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ МЕДИА

В.А. Минаев, Е.С. Поликарпов, А.В. Симонов

Цель исследования состоит в разработке методики и поиске эффективного алгоритма выявления деструктивного контента в кратких публикациях и комментариях в социальных медиа. Проведен обзор существующих решений для выявления деструктивного контента, описаны их преимущества и недостатки в контексте решаемой задачи. Сформированы составные экспериментальные корпуса текстов по темам: реабилитация нацизма, антисемитизм, радикальный ислам. Проведена нормализация корпусов, используя методы стемминга и лемматизации. Осуществлена операция векторизации нормализованных корпусов методами мешка слов (BoW), TF-IDF и слоем искусственных нейронных сетей (ИНС). Построены архитектуры глубинных ИНС: сверточной нейронной сети (CNN), рекуррентной нейронной сети с долгой краткосрочной памятью (LSTM), рекуррентной нейронной сети с механизмом вентилей (GRU). Проведены эксперименты по классификации сформированных корпусов текстов с использованием созданных ИНС и традиционных методов машинного обучения. Произведена интерпретация полученных результатов экспериментов и обосновано применение глубинных ИНС при решении поставленной задачи. Сделан вывод о целесообразности использования полученных результатов структурами, занятыми выявлением и удалением деструктивного контента.

Ключевые слова: информационная безопасность, социальные медиа, деструктивный контент, нейронные сети, глубокое обучение, классификация текста.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ КАРТОГРАФИИ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА. ЧАСТЬ 1

А.Л. Сердечный

Для определения понятия «информационная карта» осуществлен обзор основных этапов развития картографии в качестве инструментария, используемого для ориентации в окружающем пространстве, познания и планирования различных процессов, связанных с пространственными данными. С учетом данного обзора информационная карта определяется как цифровой объект, представляющий в пространстве исследуемое множество объектов, субъектов и процессов многомерного киберпространства на основе принципов: измеримости сходства объектов; близости изображений объектов, изображения контекста, воспроизводимости операций построения карты. Приводятся разноплановые примеры использования информационной карты в биологии, медицине, химии, социологии, интеллектуальном сотрудничестве и исторической науке. Тем самым обосновывается целесообразность информационного картографирования защищаемого киберпространства.

Ключевые слова: информационная карта, киберпространство, картография киберпространства.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ КАРТОГРАФИИ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА. ЧАСТЬ 2

А.Л. Сердечный

В работе типизированы задачи, для решения которых могут эффективно использоваться информационные карты, включая: разведку (исследование новых территорий, выявление скрытых элементов, установление противоборствующих сторон); планирование операций (анализ ресурсов сторон конфликтов, прокладка маршрута, прогнозирование последствий); мониторинг обстановки (координация взаимодействия, выявление изменений обстановки, вскрытие ошибок и дезинформации); представление знаний (обучение, структурированное хранение знаний, поиск информации). Рассматривается вербальная модель процесса информационно-картографического исследования. Обсуждаются методические и инструментальные аспекты информационного картографирования. Формируются задачи для реализации картографического подхода, включая: обоснование правил построения и анализа информационных карт; обоснование состава и структуры системы картографирования; разработку масштабируемой информационной карты защищаемого киберпространства.

Ключевые слова: картографическая разведка, информационная карта, картография киберпространства.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА – ПОДХОДЫ, ТЕХНОЛОГИЯ (ЧАСТЬ 1)

П.Ю. Филяк, И.А. Захаренков, И.С. Перевезенцев

В статье рассматривается подход к обеспечению информационной безопасности с позиций нового технологического уклада, основанного на широком использовании целого спектра современных методов и инструментов, характерных для информационного общества не в фазе его формировании, а на этапе интенсивного развития. Всемирный экономический форум в Давосе в 2016 году в докладах участников и итоговых документах обозначил и провозгласил четвертый технологический уклад, или инновационную экономику, также широко известную под брендом Индустрия 4.0. В технологическом плане это означает широкое использование одного из основных научно-технических направлений данного уклада – искусственного интеллекта (ИИ, Artificial Intelligence (AI)). Комплексная цифровая трансформация экономики и социальной сферы предусмотрена национальным проектом «Цифровая экономика Российской Федерации», отдельным разделом которой является обеспечение информационной безопасности цифровой экономики, что также предусматривает применение новых подходов и инструментов для решения данных задач, среди которых предусмотрено использование искусственного интеллекта.

Ключевые слова: цифровая экономика, цифровая трансформация, информация, информационное общество, информационная безопасность, искусственный интеллект, интерфейс, политика безопасности, политики доступа, идентификация, аутентификация, распознавание речи, распознавание образов, авторизация.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА – ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ (ЧАСТЬ 2)

П.Ю. Филяк, И.А. Захаренков, И.С. Перевезенцев

Предложена практическая реализация подхода к обеспечению информационной безопасности информационной системы на основе использования политик информационной безопасности, базирующихся на применении различных вариантов всех известных политик доступа к информации, которые, в свою очередь, реализуются путем имплементации платформ самых современных интерфейсов с помощью искусственного интеллекта (ИИ/ AI). Данные интерфейсы предполагают бесконтактную идентификацию и аутентификацию пользователя, в зависимости от заданных условий политик доступа, системы, правил и средств разграничения доступа к информационной системе. В частности, предусматривается идентификация и аутентификация с использованием системы визуализации и распознавания зрительных образов, а также с помощью распознавания речи, с учетом тембральных и модуляционных характеристик голоса, что обеспечивает высокую точность идентификации и аутентификации и степень достоверности при выполнении процедура авторизации, поскольку программная и аппаратная составляющая функций ИИ позволяет осуществлять многофакторный мониторинг за действиями пользователей и сортировать события в режиме online.

Ключевые слова: информация, информационное общество, информационная безопасность, цифровая экономика, искусственный интеллект, интерфейс, политика безопасности, политики доступа, идентификация, аутентификация, распознавание речи, распознавание образов, авторизация.

МЕТОДИКА ОПРЕДЕЛЕНИЯ ЦЕННОСТИ ЗАЩИЩАЕМЫХ АКТИВОВ ДЛЯ АУДИТА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

О.М. Голембиовская, К.Е. Шинаков, Е.В. Кондрашова, А.П. Жолнеров

В статье рассматривается методика, связанная с определением ценности активов для аудита обеспечения информационной безопасности коммерческой организации. Помимо этого, предложен подход для прогнозирования нанесения возможного ущерба рассматриваемым активам. Предлагаемую методику целесообразно применять службам безопасности предприятия с целью выявления недостатков системы защиты и выполнению различных мер по нейтрализации или минимизации вероятности реализации возможных угроз. Определение ценности активов организации является важным этапом аудита. Основными активами коммерческой организации с точки зрения обеспечения информационной безопасности являются: информационная система, сервер, компьютеры и иное оборудование для работы сотрудников, внутренние базы данных. Процедура определения ценности активов описана отдельно для каждого из них.

Ключевые слова: коммерческая организация, актив, ущерб, информационная безопасность, защита информации.

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДВУХЭТАПНОЙ МОДЕЛИ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ СЕТЕВЫХ АВТОМАТИЗИРОВАННЫХ СТРУКТУР

А.И. Шеншин, Е.А. Шварцкопф, К.А. Разинкин

В последние годы отмечается стремительный рост количества атак на информационные системы и ресурсы с использованием вредоносного кода и контента. Наряду с этим, происходит непрерывное совершенствование функциональных возможностей вирусов, позволяющих скрывать своё присутствие в системе. К сожалению, существующий арсенал моделей эпидемических процессов не позволяет эффективно учитывать период скрытого распространения инфекции с последующим реагированием систем защиты при практическом моделировании сетевых эпидемий. В представленном исследовании проведён анализ существующего методического обеспечения в области сетевой эпидемиологии и предложено описание (включая научно-методическое обоснование) дискретной двухэтапной модели эпидемического процесса, призванной разрешить указанное противоречие, а также - разработана методика построения этой модели, включающая соответствующие аналитические выражения для параметров моделирования.

Ключевые слова: вредоносный код, вредоносный контент, сеть, эпидемический процесс, информационно-телекоммуникационные сети, двухэтапные модели, риск.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АНАЛИЗА ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СЦЕНАРИЕВ КОМПЬЮТЕРНЫХ АТАК

С.С. Куликов, Н.Н. Мурзинов

В данной статье представлено описание принципов построения и функционирования, а также некоторые архитектурные особенности специального программного обеспечения, которое может использоваться для анализа защищённости информационных систем на основе базы данных паттернов (шаблонов) компьютерных атак, характерных для определенных типов нарушителей и их групп. Задача анализа защищенности является важным этапом работ по защите информации как при формировании требований по защите информации, так и при оценке эффективности уже реализованных мер. Ввиду нетривиального, а в какой-то мере и даже творческого характера, решение данной задачи требует высокой квалификации от специалиста, значимых временных и материальных затрат. Вследствие это возникает объективная задача по автоматизации такой деятельности. В работе описана попытка решения указанной задачи на основе разработки программного обеспечения, использующего данные из открытых источников, обобщающих опыт и квалификацию специалистов информационной безопасности из разных стран.

Ключевые слова: анализ защищенности, информационная система, открытые данные.