ВЫЯВЛЕНИЕ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ МЕДИА НА ОСНОВЕ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

В.А. Минаев, А.Д. Реброва, А.В. Симонов

В статье обсуждаются модели классификации текстового контента и методы его предварительной обработки с целью выявления деструктивных воздействий в социальных медиа. Показано, что основным источником деструктивного контента выступает профиль пользователей, характеризующийся набором личным данных, содержанием публикаций, параметрами сообщества, аккаунтов сети, сообщений и чатов. Говорится об актуальности автоматизированного сбора и анализа данных с помощью моделей прецедентного и дедуктивного обучения. Рассматриваются их основные разновидности и задачи, решаемые на их основе, включающие прогнозирование и типологизацию в аспекте деструктивного содержания текстов, снижение размерности признаков их описания. Исследованы и применены основные методы векторизации текстов: Bag of Words, TF_IDF, Word2vec. На практических корпусах текстов из социальной сети ВКонтакте решены задачи выявления деструктивного контента, связанного с радикальным исламом. Показано, что с помощью примененных моделей и методов все тексты, включающие деструктивный контент, классифицированы верно. Наиболее высокую точность (0,97) при решении задачи распознавания деструктивного контента дает системная интеграция алгоритма векторизации Bag of Words, метода главных компонент для снижения пространства признаков описания текстов и логистической регрессии или случайного леса как моделей обучения. Сделан вывод, что наборы данных, имеющие связь с исламским радикализмом, характеризуются достаточно четкими признаками, которые хорошо вычисляемы с помощью современных моделей, методов и алгоритмов, и могут эффективно применяться для автоматизированной классификации текстовых массивов с целью выявления их деструктивной направленности. Развитие направления, представленного в статье, связано с увеличением исследуемых корпусов документов, более детальным анализом текстов на основе сложных моделей распознавания латентной экстремистской пропаганды, в том числе – представленной в фото, аудио- и видеоформатах.

Ключевые слова: деструктивный текстовый контент, исламский радикализм, социальные медиа, распознавание негативного информационного воздействия, модель машинного обучения.

ОСОБЕННОСТИ РАЗМЕЩЕНИЯ БАЗ ПЕРСОНАЛЬНЫХ ДАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НАУЧНО-ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

П.Ю. Пушкин

В статье проведен анализ нормативных актов по организации обработки и защите персональных данных на предмет размещения баз данных, используемых в информационных системах российских учреждений научно-образовательной сферы. С 2015 года законодательством Российской Федерации определена необходимость размещения баз персональных данных на территории нашей страны. Однако есть случаи, когда хранение персональных данных возможно и за пределами нашей страны. В работе рассмотрены такие исключения, применимые к сфере деятельности научно-образовательных учреждений. На основе автоматизированного анализа реестра операторов персональных данных определено соотношение высших учебных заведений, представивших сведения о месте нахождения своих баз данных в соответствии с Российским законодательством. Более 24% высших учебных заведений такие сведения не предоставили, что может говорить о необходимости оказания университетскому операторскому сообществу методической помощи по вопросам порядка обработки и защиты персональных данных. В ходе проведения контроля за порядком обработки персональных данных по требованию Роскомнадзора необходимо представить, в том числе, документы, подтверждающие расположение баз персональных данных информационных систем в пределах границ Российской Федерации. В работе разработаны рекомендации по размещению и документальному оформлению местонахождения баз данных, использующихся в информационных системах научно-образовательных учреждений, при использовании собственной и предоставляемой третьими лицами ИТ-инфраструктуры.

Ключевые слова: защита персональных данных, защита баз данных, персональные данные, реестр операторов персональных данных.

ФОРМАЛИЗАЦИЯ ПОДХОДА К ОПРЕДЕЛЕНИЮ УРОВНЯ МОТИВАЦИИ НАРУШИТЕЛЯ

О.М. Голембиовская, Е.В. Кондрашова, М.Ю. Рытов, М.М. Голембиовский

В статье рассматривается подход, связанный с определение уровня мотивации нарушителя к совершению того или иного противоправного деяния относительно ресурсов организации. Предлагаемый подход, возможно, применять службам безопасности предприятия относительно работников как при приеме на работу, так и в процессе работы с целью выявления высокого уровня мотивации к совершению противоправного деяния и выполнению различных мер по нейтрализации или минимизации данного уровня. Уровень мотивации напрямую влияет на потенциал нарушителя и на вероятность реализации им угрозы, так как не только наличие на объекте средств защиты или наличие у нарушителя современных средств атак приводит к реализации угрозы. В первую очередь к ней приводит заинтересованность в совершении данного деяния, мотивируемость и цели, которые преследует нарушитель.

Ключевые слова: модель нарушителя, мотивация, лояльность, информационная безопасность, защита информации.

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ КОМПЬЮТЕРНЫХ АТАК, РЕАЛИЗУЕМЫХ ГРУППИРОВКОЙ APT3 В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.Л. Сердечный, А.В. Айдаркин, М.А. Тарелкин, А.Е. Дешина

В работе представлены результаты моделирования способов реализации долговременных целенаправленных атак на корпоративные распределённые компьютерные системы со стороны одной из опасных киберпреступных группировкок – Advanced Persistent Threat 3 (APT3). Осуществлено моделирование способов, реализуемых APT3. Построение моделей осуществлялось с использованием аппарата сетей Петри на основании сведений о технических приёмах, содержащихся в базе данных MITRE ATT&CK. Разработанные модели взаимосвязаны по условиям и последствиям реализации основных технических приёмов, актуальных для корпоративных распределённых компьютерных сетей. Реализованный подход также позволяет моделировать меры защиты, регламентируемые нормативными и методическим документами, что даст возможность принятия обоснованных решений при построении системы защиты с учётом специфики защищаемого объекта.

Ключевые слова: киберпреступные группировки, APT-атаки, сети Петри, ATT&CK, APT 3, распределенные компьютерные системы.

ОЦЕНКА СТОЙКОСТИ ПОТОЧНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, ФУНКЦИОНИРУЮЩИХ В СОСТАВЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ

Н.М. Радько, С.С. Тихонова, А.Н. Мокроусов

Целью исследования является повышение защищенности телекоммуникационных систем управления в контексте криптографической защиты с использованием математического аппарата риск-анализа для оценки стойкости поточных криптосистем. Стойкость поточной криптосистемы в работе рассмотрена как совокупность рисков разнородных компонентов поточной криптосистемы, уязвимых к деструктивному воздействию. В ходе исследования проанализированы уязвимости компонентов поточной криптосистемы, особенности среды функционирования, построены модель угроз и риск-модель атакуемой поточной криптосистемы, предложены мероприятия по снижению рисков поточных криптосистем. Полученные результаты могут быть использованы или адаптированы при необходимости повышения стойкости поточных криптосистем на этапах проектирования и модернизации, а также при необходимости восстановления эффективности функционирования после компрометации или взлома. На основе предложенной риск-модели поточной криптосистемы в дальнейшем возможна реализация программного обеспечения для оценки стойкости поточных криптосистем.

Ключевые слова: поточная криптосистема, уязвимость, угроза, риск.

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА КОРПОРАТИВНЫЕ РАСПРЕДЕЛЕННЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ

А.Л. Сердечный, А.А. Шевелюхин, М.А. Тарелкин, А.В. Бабурин

В настоящей статье представлены результаты моделирования способов реализации компьютерных атак на корпоративные распределенные компьютерные системы. Предложенные модели способов предназначены для формирования методического обеспечения расчета рисков и выявления оценки защищенности таких систем от актуальных сценариев реализации угроз безопасности информации, которое даёт возможность обоснованного выбора мер защиты. Построение моделей способов реализации компьютерных атак осуществлялось с использованием аппарата сетей Петри на основании сведений, содержащихся в базе данных MITRE ATT&CK. Разработанные модели взаимосвязаны по условиям и последствиям реализации основных технических приёмов, определённых в базе данных ATT&CK и актуальных для корпоративных распределённых компьютерных сетей (условия и последствия моделируются позициями сети Петри, а сами технические приёмы – переходами сети Петри). Также в статье продемонстрирована возможность наращивания модели за счёт включения в неё моделей мер защиты, используемых в нормативных и методических документах ФСТЭК России.

Ключевые слова: корпоративные распределённые компьютерные систем, способы реализации компьютерных атак, ATT&CK, сети Петри, моделирование мер защиты.

РАЗРАБОТКА СРЕДСТВ МАСКИРОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ ПОДВИЖНОЙ ЦИФРОВОЙ ЗАЩИЩЕННОЙ СВЯЗИ

Н.М. Радько, А.А. Караханова

Целью исследования является повышение защищенности цифровых данных, передаваемых в телекоммуникационных сетях подвижной цифровой защищенной связи от атак, нацеленных на нарушение конфиденциальности этих данных, за счет создания соответствующего методического обеспечения оценки и регулирования рисков успешности вышеупомянутых атак. В работе проводится анализ алгоритмов и методов, используемых злоумышленниками в ходе организации и проведения атак на защищаемые цифровые данные. Полученные результаты могут быть использованы как для более эффективной информационной защиты цифровых данных в телекоммуникационных сетях подвижной цифровой защищенной связи, так и как базис для дальнейших исследований.

Ключевые слова: телекоммуникационная сеть, цифровые данные, информационная безопасность.

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ КОМПЬЮТЕРНЫХ АТАК, РЕАЛИЗУЕМЫХ ГРУППИРОВКОЙ APT29 В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.Л. Сердечный, П.С. Краюшкин, М.А. Тарелкин, Ю.К. Язов

Статья посвящена моделированию компьютерных атак на распределённые корпоративные компьютерные системы, на примере действий группировки Advanced Persistent Threat 29 (APT29). В статье предлагается подход моделирования способов, реализуемых указанной группировкой, а также мер защиты от них. Подход основан на использовании аппарата сетей Петри, а также сведений о технических приёмах, предоставляемых в рамках проекта MITRE ATT&CK. Разработанные модели учитывают связи по условиям и последствиям действий, совершаемых группировкой APT29 в ходе атак на распределённые корпоративные системы. Также в статье продемонстрирована возможность наращивания модели за счёт включения в неё

моделей мер защиты от рассмотренных способов реализации компьютерных атак. Предлагаемые модели могут быть дополнены за счёт моделирования новых способов реализации компьютерных атак, используемых другими кибергруппировками. Кроме того, модели могут быть расширены до моделей сети Петри-Маркова путём реализации частным методик расчёта вероятностно-временных характеристик для фрагментов предлагаемых моделей.

Ключевые слова: киберпреступные группировки, APT-атаки, сети Петри, ATT&CK, APT 29, распределенные компьютерные системы.

РАСЧЕТ РИСКОВ И ОЦЕНКА УГРОЗ ИСПОЛЬЗОВАНИЯ СИСТЕМ ГОЛОСОВОГО УПРАВЛЕНИЯ В ДОВЕРЕННЫХ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.А. Хайдаров, А.С. Шишлов, Н.Н. Толстых

Цель исследования состоит в повышении защищенности элементов распределенной компьютерной системы автоматического распознавания голосовых команд от возможного неверного определения команды за счет создания алгоритмического обеспечения оценки и регулирования рисков неверной идентификации голосовой команды для сравнения реализации двух алгоритмов: алгоритм динамической трансформации временной шкалы и алгоритм на основе скрытых Марковских процессов.Полученные результаты могут быть использованы или адаптированы при необходимости повышения стойкости систем автоматического распознавания голосовых команд на этапах проектирования и модернизации, а также при необходимости восстановления эффективности функционирования после компрометации или взлома.

Ключевые слова: искусственный интеллект, распознавание речи, уязвимость, угроза, риск.

РАЗРАБОТКА МЕТОДИЧЕСКОГО АППАРАТА ВНЕДРЕНИЯ ЗАЩИТНЫХ ФУНКЦИЙ В ОТЕЧЕСТВЕННЫХ МИКРОКОНТРОЛЛЕРАХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ПОДВИЖНОЙ ЦИФРОВОЙ ЗАЩИЩЕННОЙ СВЯЗИ

А.И. Мордовин, Д.С. Хохлова

Целю исследований является повышение защищенности данных и программного кода Flash – памяти отечественных микроконтроллеров в телекоммуникационных системах (ТКС) цифровой подвижной защищенной связи от атаки программного обеспечения (несанкционированного доступе и копирование) за счет регулирования рисков успешности вышеуказанной атаки путем разработки методического аппарата защиты кода программ. В работе продемонстрирован программный метод с использованием bootloader – загрузки программы из внешней памяти. Проведен анализ спецификаций на отечественные и зарубежные микроконтроллеры. Полученные результаты работы могут послужит обеспечению безопасности отечественных микроконтроллеров и дальнейшему развитию способов противодействия угрозам. Разработанный методический аппарат защиты кода программ от несанкционированного доступа позволит вывести отечественное оборудование на должный уровень применения, что позволит провести политику импортозамещения в части защиты кода программ.

Ключевые слова: микроконтроллер, защитные функции, микросхема памяти, доступ к внешним интерфейсам.

ОЦЕНКА РИСКОВ УСПЕШНОЙ РЕАЛИЗАЦИИ СПУФИНГ-АТАК НА ЭЛЕМЕНТЫ ГОЛОСОВОЙ АУТЕНТИФИКАЦИИ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А. А. Хайдаров, С. А. Бодячевский, Н. Н. Толстых

Цель исследования заключается в рекомендациях по улучшению мер защиты голосовых систем аутентификации от реализации спуфинг-атак. В работе рассмотрены разнообразные виды спуфинг-атак и выделены самые опасные на данный момент. Разработана методика оценки защищенности голосовых систем аутентификации, учитывающая воздействие различных видов спуфиг-атак на системы голосовой аутентификации. Проведены количественные эксперименты, показывающие преимущество разработанной методики, в сравнении с существующими аналогами. Описан комплекс программных средств оценки защищенности систем голосовой аутентификации, который позволяет автоматизировать процесс оценки при проведении технологических испытаний. Полученные результаты могут быть использованы не только для оценки защищенности систем голосовой аутентификации, но и для проведения функционального и нагрузочного тестирования. Применение предложенного комплекса и методики оценки в дальнейшем может помочь в разработке технических решений по увеличению защищенности голосовых биометрических систем от реализации спуфинг-атак.

Ключевые слова: оценка рисков, спуфинг-атаки, голосовая аутентификация.

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ СЕТЕЙ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ НА РАЗНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА СИСТЕМ В УСЛОВИЯХ ОТСУТСТВИЯ СТАТИСТИКИ УЩЕРБА

С.А. Ермаков, С.Ю. Громовиков, А.А. Болгов, Е.А. Москалева

В данной статье предлагается методика количественной оценки рисков успешной реализации атак, направленных на нарушение конфиденциальности данных на этапе проектирования систем, основанная на применении нейро-нечетких сетей. Представлен программный инструментарий, для выбора оптимальной конфигурации системы, который позволяет выбирать и сравнивать различные конфигурации выбранных устройств, и как итог, выбрать наиболее оптимальную для себя конфигурацию. Получена методика количественной оценки риска на этапе начала эксплуатации систем в условиях отсутствия статистики ущерба, несмотря на качественный характер входных параметров, оцененных экспертами. Данная методика основана на многокаскадном применении логического интерфейса Мамдани. Декомпозиция оцениваемых параметров позволяет уменьшить влияние субъективных оценок экспертов на исследуемый объект. Предложенная методика реализована с помощью имитационного программного комплекса.

Ключевые слова: промышленный интернет вещей, сеть, риск, экспертные оценки, нечеткие множества, эффективность, защищенность.

ПРИНЦИПЫ УПРАВЛЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМИ СТРУКТУРАМИ ПРИ ИНФОРМАЦИОННЫХ РЕСТРИКЦИЯХ В УСЛОВИЯХ ПАНДЕМИИ

В.А. Минаев, К.М. Бондарь

В статье рассматривается применение ментальных карт для решения проблем обеспечения В статье рассматривается новый сетецентрический подход к управлению социальными и экономическими структурами в условиях пандемических ограничений, базирующийся на применении современных информационных технологий и сетевой организации информационного обмена. Рассматриваются информационно связанные структуры, состоящие из малых и средних предприятий, а также различных сообществ (молодежь, пенсионеры, профессиональные и иные организации). Обсуждается принцип самосинхронизации и вводится понятие “аттрактор” при сетецентрическом построении управления такими структурами. Обосновывается приоритет стратегии “заимствования” при применении механизмов диффузии инноваций в экономику и социальную жизнь регионов России. Предлагается полисетевая схема инновационного развития социально-экономической сферы. Она дает возможность построить инновационную инфраструктуру с применением достижений в разработке бизнес-сетей сотрудничества, а также моделей активного воздействия на общественное сознание в социальных сетях. Показана важная роль математических моделей распространения информации в социальных сетях с учетом территориальных различий для эффективного управления социально-экономическими структурами в регионах России в условиях пандемии. Найдены динамические функциональные зависимости, позволяющие отделять одни поселения от других по степени восприимчивости населения к информационному воздействию социально-экономического характера в социальных сетях, что дает возможность целенаправленно строить и реализовывать как экономические, так и социальные программы, бизнес-политику в том или ином кластере. Полученное географически компактное распределение поселений по кластерам дает возможность углубленного исследования причин региональных различий скорости распространения информации, что открывает способы оптимального информационного воздействия на региональную экономику, образовательную систему, бизнес-структуры, социальные образования (сообщества пенсионеров, молодежные структуры, клубы по интересам и т. п.) с целями их консолидации, перевода на инновационные пути развития, выработки перспективных средств и методов ведения бизнеса, стимулирования экономики в сложных условиях пандемической ситуации.

Ключевые слова: социальные и экономические структуры, сетецентрическая модель управления, пандемия, информационные технологии, самосинхронизация, аттрактор, стратегия “заимствования”, образовательный сегмент, кластер.

ПРИМЕНЕНИЕ СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТКС

П.Ю. Филяк, А.Н. Ермолин, Д.С. Семяшкина, М.А. Корецкий, И.С. Колобов

В статье рассматриваются организационно-технологический и инженерно-технический методы защиты информации и их инструменты – средства защиты информации (СЗИ) для обеспечения информационной безопасности информационно-телекоммуникационной сети (ИТКС), к каковым можно отнести любую корпоративную информационную систему (КИС). При всей кажущейся на первый взгляд простоте данный тип задач нельзя никоим образом отнести к тривиальным, поскольку, с одной стороны, применяемые СЗИ представляют собой сертифицированные решения с совершенно определенными диапазонами технических и технологических параметров, что требует весьма непростой и точной настройки и адаптации, с другой стороны, комплексная защита информации требует применения различных СЗИ, отличающихся не только своими характеристиками, но производителями, что автоматически генерирует целый спектр дополнительных задач, а зачастую даже проблем.

Ключевые слова: информация, защита информации, информационно-телекоммуникационная сеть (ИТКС), средства защиты информации (СЗИ), информационная безопасность.