КАРТОГРАФИЧЕСКОЕ ИССЛЕДОВАНИЕ BLOCKCHAIN-ТРАНЗАКЦИЙ И СМАРТ-КОНТРАКТОВ КИБЕРПРЕСТУПНИКОВ, АТАКУЮЩИХ АВТОМАТИЗИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ, И ОЦЕНКА УЩЕРБОВ ОТ РЕАЛИЗАЦИИ ИХ АТАК

А.Л. Сердечный, Д.А. Скогорева, Е.П. Длинный, Т.Ч. Ле, Д.В. Чьеу

Целью настоящих исследований следует считать противодействие компьютерной преступности за счёт совершенствования методов анализа их финансовых транзакций, осуществляемых в рамках операций с криптовалютами, построенными по технологии Blockchain. В рамках исследований разработана программная система сбора и картографического анализа сведений о Bitcoin-транзакциях и смарт-контрактах, а также разработана методика её применения для решения задач, связанных с противодействием компьютерной преступности. На примере анализа деятельности криптовымогателей показана возможность использования методики для оценки рисков, связанных с соответствующими угрозами. На основании полученных оценок были разработаны рекомендации по снижению рисков от угроз воздействия криптовымогателей. Полученные результаты могут быть применены для противодействия компьютерным преступлениям на корпоративные информационные системы, а также для оценки рисков реализации других угроз, связанных с группировками, использующими криптовалюты для осуществления своей преступной деятельности.

Ключевые слова: картографический метод, Blockchain, смарт-контракты, Bitcoin, криптовымогатели, риск, ущерб.

АЛГОРИТМИЧЕСКОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РИСК-АНАЛИЗА АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «УМНЫЙ ДОМ»

С.А. Ермаков, К.Н. Петрухненко, А.А. Болгов, А.Н. Бартенев

В работе проводится сравнительный анализ существующих методик оценки и регулирования рисков, а также изучается возможность их применения в условиях использования сетей устройств умного дома в контексте их использования при проведении оценки и регулирования рисков. Предлагается оригинальная методика риск-анализа в сетях устройств умного дома, повышающая степень защищенности таких систем, которая основана как на использовании наиболее подходящих процедур из рассмотренных методик, так и на использовании аппарата нечётких чисел. Произведена первоначальная классификация угроз для систем умного дома. Разработана последовательность вычислений для типовых систем и система ввода данных, позволяющая пользователю самостоятельно задавать параметры для модели сети, что обеспечивает наибольшую точность при проведении оценки и регулировании рисков. Предложенная модель реализована при помощи разработанного программного комплекса.

Ключевые слова: риск, интернет вещей, умный дом, нечёткие числа, сетевая атака, уязвимость.

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ РЕАЛИЗАЦИИ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ДАННЫМ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «УМНЫЙ ДОМ»: МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

В.Е. Кунавин, С.А. Ермаков, А.А. Болгов, С.В. Лихобабин

В работе проводится разработка методического подхода и программного обеспечения оценки и регулирования рисков реализации угроз несанкционированного доступа к данным автоматизированной информационной системы «Умный дом». Предлагается оригинальный подход к анализу защищенности таких систем, основанный на применении аппарата теории рисков и нечёткой логики. Произведен анализ существующих подходов к обеспечению безопасности информационных систем. Построена методическая база оценки рисков и рекомендации по их регулированию. Предложенный методический подход реализован с помощью имитационного программного комплекса. Предложена методика регулирования рисков, основанная на анализе состояния межмашинного взаимодействия внутри сети с течением времени. Произведена оценка эффективности методического подхода к оценке и управлению рисками.

Ключевые слова: риск, интернет вещей, умный дом, нечёткая логика, сетевая атака.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОВИД-ИНФОДЕМИИ

И.В. Щетинина, Е.А. Москалева, М.Е. Волкова, В.К. Власов

Цель исследования состоит в разработке методики и поиске эффективного алгоритма Инфодемия представляет собой стремительное и неконтролируемое распространение в медиа необоснованной и ложной информации о кризисных событиях. Во время пандемии коронавируса возникла новая разновидность сетевой дезинформации, связанная с распространением различных слухов о заболевании, вакцинации и т. п., которая стремительно развиваясь, охватила все страны, став таким образом ковид-инфодемией. Инфодемия наносит большой вред работе систем здравохранения, правительств стран, существенно снижая уровень доверия к ним граждан. В статье представлена математическая модель инфодемии, основанная на данных по статистике о слухах, посвященных коронавирусной пандемии. За основу взяты эпидемические SEIR и SEIR-D модели. Результаты моделирования показали применимость предлагаемых моделей. Предлагаемые в статье модели можно использовать для прогнозирования развития и моделирования угроз ковид-инфодемии, в задачах определения ущерба, наносимого ковид-инфодемией экономике и здравохранению.

Ключевые слова: инфодемия, эпидемическая модель, информационная безопасность, коронавирусная инфодемия.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО ПРОГРАММНОГО МОДУЛЯ РЕГИОНАЛЬНОГО ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯ

А.Ю. Каушан, А.В. Поздникина, А.Г. Остапенко, А.С. Пахомова, И.А. Боков

В статье рассмотрена корреляция факторов влияния на уязвимость к деструктивному контенту в социальных сетях и параметров интернет-пользователя. В этой связи авторами предлагается методология, а также программная реализация, позволяющая определять подверженные деструктивному воздействию в сети страты региональных интернет□пользователей. Практический смысл предлагаемой работы заключается в том, что благодаря данной методологии появилась возможность на основе социального опроса пользователей интернет пространства с помощью статистической вероятности оценить шанс попадания под негативное воздействие деструктивного контента. При достаточной общности предлагаемой методики акцент сделан на региональный аспект. Все это в совокупности образует полную методологию, которая может служить основой для дальнейших исследований, проводимых в данной сфере, а также использоваться для выработки рекомендации по снижению уязвимости пользователей регионального интернет-пространства от влияния деструктивного контента.

Ключевые слова: социальная сеть, деструктивный контент, безопасный интернет.

РИСК-МОНИТОРИНГ КОММЕНТАРИЕВ В АВТОМАТИЗИРОВАННЫХ СОЦИАЛЬНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А.Г. Остапенко, А.С. Пахомова, М.В. Лопатченко, Е.Ю. Чапурин, Т.Ю. Мирошниченко

Цель исследования заключается в повышении защищенности пользователей автоматизированной социальной сети «ВКонтакте» за счет использования алгоритма проведения риск-мониторинга комментариев, оставленных на публикуемый контент деструктивной направленности, с использованием средств искусственного интеллекта. Разработан возможный алгоритм риск-мониторинга комментариев с использованием средств искусственного интеллекта, позволяющий самостоятельно определять комментарии, имеющие деструктивную направленность. Алгоритм разработан с целью повышения защищенности пользователя от влияния контента деструктивной направленности в онлайн-сообществах города Воронеж, а также для дальнейшего его внедрения в программный продукт «Netepidemic-CMSN». Для его реализации были определены наиболее подходящие методы машинного обучения алгоритма, разработана метрология комментариев в автоматизированной социальной сети, а также процесс обработки данных, благоприятный для эффективного обучения алгоритма искусственного интеллекта. Также представлено информационное и алгоритмическое обеспечение разработанного метода.

Ключевые слова: автоматизированная социальная сеть, онлайн-сообщества, риск-мониторинг, искусственный интеллект, контент.

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЛЕКСА МОДЕЛИРОВАНИЯ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ С УЧЕТОМ ДОЗИРОВКИ ВИРУСОВ: МОДЕЛЬ «БАХЧИСАРАЙСКИЙ ФОНТАН»

А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, В.В. Сафронова, К.В. Сибирко, Е.А. Болгова

В работе предлагается принципиально новый подход к описанию сетевых эпидемических процессов. Авторы предлагают при моделировании процесса диффузии вредоноса учитывать его дозировку в элементах исследуемой сети. В этой связи вводятся соответствующие параметры (скорость размножения вируса, пороги концентрации вируса в узлах сети по состояниям распространения вредоноса и утраты работоспособности, пропорция дозировки вируса в сетевых трафиках), которые через заданные матрицы ресурсов взвешенной сети позволяют моделировать процесс распространения инфекции по сетевой инциденции (вплоть до программной реализации). Наряду с вышеизложенным рассматриваются приемы регулирования эпидемического процесса в предлагаемом авторами прочтении.

Ключевые слова: сеть, вирус, эпидпроцесс, ресурс, потенциал, вершина и дуга сети.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ АКТИВОВ

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков

Рассматривается подход к обеспечению информационной безопасности организации с позиций системного и процессного подходов, отраженных в серии государственных стандартов, посвященных менеджменту (управлению) в сфере информационной безопасности, в основе которого находится политика информационной безопасности и, соответственно, политика доступа к информации, реализация которой начинается прежде всего с оценки информационных активов (Asset), информационных ресурсов (Assets), а затем и управления ими (Asset Management) с позиций информационной безопасности. Оценка информационных активов начинается прежде всего с их инвентаризации, для которой необходимы программно-аппаратные средства (инструментальные средства), адекватно и эффективно выполняющие указанную функцию. К таковым инструментам можно, в частности, отнести Total Network Inventory 5 (TNI) - быстрая инвентаризация сетевых компьютеров, оборудования, программного обеспечения и комплексный программный продукт Algorius Net Viewer - для мониторинга и инвентаризации, визуализации, администрирования, компьютерной сети любого уровня.

Ключевые слова: информация, информационная безопасность, политика безопасности, политики доступа, инвентаризация, информационный актив, информационные ресурсы, интерфейс, протокол, IP – маршрутизация, трассировка маршрута, сканирование портов, опрос устройств.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ФОРЕНЗИКИ

П.Ю. Филяк, С.В. Королев, Н.В. Тебеньков

Представлен подход к обеспечению информационной безопасности [1] с помощью применения инструментальных средств прикладной науки о расследовании и раскрытии преступлений, связанных с компьютерной безопасностью, известной под названием форензика. Рассматриваются кратко терминология, теоретические основы и подходы данной науки, а также представлен набор конкретных инструментов для реализации форензики в рамках программно-аппаратных комплексов, которые можно применять на практике в целях обеспечения информационной безопасности коммерческих и не коммерческих организаций, а также иных субъектов экономической деятельности. Представлены три программных продукта: OSForensics - комплект утилит для проведения компьютерной экспертизы, выполняющий поиск и анализ различных данных в системе, восстанавливающий данные, предоставляющий возможность просмотра следов активности пользователя; Belkasoft Evidence Center - инструмент для комплексной цифровой криминалистической экспертизы и расследования корпоративных инцидентов и Passware Kit Forensic – инструмент для поиска всех зашифрованных файлов на носителях информации.

Ключевые слова: информация, информационная безопасность, политика безопасности, политики доступа, интерфейс, идентификация, аутентификация, форензика, драйвер, утилита, дамп, анализ, пароли, стойкость паролей, событие информационной безопасности, инцидент информационной безопасности, handshake.

АНАЛИЗ ДОВЕРИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИОННОГО РЕСУРСА АВТОМОБИЛЯ НА ОСНОВЕ НАВИГАЦИОННОГО КЛЮЧА

Т.З. Аралбаев, Р.Р. Галимов, А.И. Сарайкин

В статье определена актуальность задачи обеспечения информационной безопасности информационного ресурса (ИР) автомобильных транспортных средств (АТС), обусловленная увеличением степени использования информационных технологий в современных транспортных средствах и наличием уязвимостей в штатных средствах защиты. Проведен обзор литературы и выявлены недостатки существующих решений систем защиты доступа (СЗД) к ИР АТС. Определена перспективность подхода к защите ИР АТС, учитывающего взаимное расположение субъекта и объекта доступа. Предложена формализованная процедура оценки доверия к многоуровневой системе защиты доступа к ИР АТС на основе навигационного ключа, учитывающая характеристики и условия эксплуатации информационной системы, требования защиты, текущую конфигурацию мер и средств защиты. Представлены алгоритмическая модель и метод оценки доверия к системе защиты на основе системы признаков и кодов защиты. Приведены расчеты оценки доверия к системе защиты ИР автомобиля.

Ключевые слова: система разграничения доступа, информационный ресурс, автомобильное транспортное средство, навигационный ключ, система признаков, код защиты.

АНАЛИЗ СОВРЕМЕННЫХ ТОЧЕК ДОСТУПА БЕСПРОВОДНЫХ КАНАЛОВ ПРЕДПРИЯТИЯ

Ю.Ю. Громов, П.И. Карасев, В.В. Кулешов

В статье дается характеристика беспроводных сетей, имеющих значение для автоматизации производства, и условия для их применения. Рассмотрено применение проводной сети Ethernet, поскольку беспроводная сеть можно с легкостью в нее интегрироваться. Проведен анализ таких распространенных в автоматизации предприятий типов стандартов связи, как ZigBee и Wi-Fi. Уделено внимание проблеме взаимодействия узлов в проводных и беспроводных сетях и возможности ее решения с использованием технологии коллективного доступа с опознаванием несущей и обнаружением конфликтов. Определено, что точки доступа являются устройствами, обладающими операционными системами, в которых содержится большое количество ошибок, чем могут воспользоваться злоумышленники. Рассмотрены основные причины взлома на примере Wi-Fi и охарактеризованы методы взлома беспроводной точки доступа. Указаны способы, которые могут применяться для защиты беспроводной точки доступа. Также проведен анализ технологий, которые могут использоваться для того, чтобы защитить корпоративные сети.

Ключевые слова: беспроводные каналы, точки доступа, хендшейк; метод с использованием фишинговой точки доступа; метод подбора WPS кода, способы защиты беспроводной точки доступа.

К ВОПРОСУ О СОЗДАНИИ ПЛАТФОРМЫ КАРТОГРАФИРОВАНИЯ РИСКОВ ЗАЩИЩАЕМОГО КИБЕРПРОСТРАНСТВА

А.Л. Сердечный, А.А. Гончаров, М.А. Булычев, А.В. Коноплин, О.С. Газизянов, Р.О. Дыкин, Д.С. Нестеров, Д.А. Нархов

Статья посвящена перспективам создания платформы картографирования рисков защищаемого киберпространства, потребность в которой обусловлена нарастанием неопределённости в отношении процессов, протекающих в киберпространстве. Наглядное представление таких процессов позволяет своевременно выявлять и провести исследование опасных тенденций для безопасности личности, общества и государства. В данной работе формулируются цели, задачи и функциональные требования к платформе картографирования рисков. Представленные результаты основаны на практическом опыте разработки и применения методологии картографирования защищаемого киберпространства, который был получен в ходе разработки системы картографирования рисков защищаемого киберпространства (прототип разрабатываемой платформы). Целью создания платформы является объединение усилий множества исследователей киберпространства благодаря обеспечению совместной работы по его представлению в виде системы взаимосвязанных информационных карт. Вниманию научной общественности предлагается облик платформы картографирования рисков защищаемого киберпространства и возможные решения, которые могут быть использованы для её воплощения в виде готового продукта.

Ключевые слова: киберпространство, картографирование защищаемого киберпространства, платформа картографирования рисков.

АНАЛИЗ РИСКОВ ПРИ ПОМОЩИ ИНФОРМАЦИОННОЙ КАРТЫ МУЗЫКАЛЬНЫХ ПРЕДПОЧТЕНИЙ

А.Л. Сердечный, Д.Г. Коденцева, А.А. Петелин, А.А. Лемешко, В.Е. Руженко

Роль количественной оценки рисков является ключевой в обоснованном принятии решений в отношении разработки мер защиты. Однако одного лишь интегрального значения, которое характеризует уровень опасности тех или иных видов угроз, недостаточно для полного понимания процессов, связанных с негативными воздействиями на защищаемые объекты. Отображение значений риска с помощью информационной карты позволяет не только оценить, но и «увидеть» уровень опасности с учётом особенностей «ландшафта» защищаемой системы. В настоящей работе демонстрируется реализация данной идеи на примере анализа риска вовлечения пользователей социальных сетей в группы единой тематики. Для расчёта риска используются сведения о музыкальных исполнителях, которых слушают пользователи социальной платформы ВКонтакте, состоящие в группах единой тематики. Для наглядного представления значений риска вовлечения пользователя в группу единой тематики в отношении каждого музыкального исполнителя проводится расчёт частных показателей риска, которые отображаются на информационной карте музыкальных предпочтений. Для её построения использованы данные рекомендательной системы музыкального сервиса Яндекс.Музыка. Также в статье продемонстрирована возможность использования информационных карт музыкальных предпочтений для составления и анализа профилей пользователей социальных платформ.

Ключевые слова: информационная карта музыкальных предпочтений, информационная безопасность, картографирование рисков, профиль пользователя, киберпространство.