Введение

Для современного этапа развития общества характерен непрерывный процесс информатизации и совершенствования информационных технологий, который обуславливает интенсивный рост информации, сосредоточенной в информационно-телекоммуникационных сетях и, как следствие, необходимость управления такой информацией при помощи различных технологий и сервисов.Одними из наиболее перспективных и востребованных телекоммуникационных сервисов становятся решения на базе M2M-технологий [1,5].

M2M объединяет телекоммуникационные и информационные технологии для автоматизации бизнес-процессов и создания более проработанных комплексов услуг. Одной из первых разработок в области M2M-технологии является решение Qualcomm разработанное для отслеживания коммерческого транспорта. На сегодняшний день M2M-технология применяется в самых различных сферах: обеспечения безопасности, автоматизации промышленных и транспортно-логистических процессов, систем слежения, контроля расхода ГСМ и др.Все больше государственных и коммерческих организаций выбирают этот инструмент для мониторинга, контроля и эффективного управления удаленными объектами в самых разных отраслях.[6,18].

Такая технология основана на использовании проводной или беспроводной связи, что позволяет M2M-компонентам напрямую взаимодействовать друг с другом. На практике M2M-технологии используют производственное и телекоммуникационное оборудование, центры обработки данных, системы хранения, устройства защиты конфиденциальности и т.д. Так, например, благодаря технологии межмашинного взаимодействия комплекс устройств, осуществляющих мониторинг городского трафика, может передавать данные на светофоры для регулирования потока автомобилей, а системы технического контроля могут получать информацию о проблемах с производственным оборудованием [3,4,19].

В связи с тем, что M2M-технология позволяет компонентам ИТКС

обмениваться информацией или же передавать ее в одностороннем порядке, технология межмашинного взаимодействия является неотъемлемой частью работы ИТКС.Кроме того,компоненты ИТКС могут не только собирать данные о других устройствах, но и на основе полученной информации предпринимать определенные действия [6,10,13].

Несмотря на широкое применение и огромный потенциал для роста применения технологии межмашинного взаимодействия в различных областях, существует широкий перечень вопросов к защищенности и безопасности использования таких технологий [7].

Одной из главных проблем, с которой сталкиваются при внедрении M2M-технологий, является возможность управления большим числом устройств с разными характеристиками без ущерба для каналов связи. На сегодняшний день экономичность передачи потоков данных, циркулирующих в ИТКС с большим количеством датчиков, является актуальной задачей, для решения которой владельцы ИТКС экспериментируют с архитектурой сети и подходами к обмену данными [11].

Дело в том, что используемые коммуникации реализованы по самым разнообразным технологиям, но все они имеют некоторые схожие черты. И наиболее важная из этих черт – изначальное отсутствие фактора защищенности в архитектуре таких систем и протоколов. В результате применения такого подхода система является уязвимой для широкого перечня сетевых атак. В таких условиях необходимо уделять особое внимание информационной безопасности применения технологий межмашинного взаимодействия [11,12].

Кроме того, необходимо учитывать тот факт, что уязвимость ИТКС существенно превышает уязвимость самих компонентов. Это связано, прежде всего, с масштабностью, открытостью и неоднородностью самих ИТКС. При этом число угроз ИБ и способов реализации сетевых атак постоянно увеличивается [11,12].

Статистика показывает, что инциденты, связанные со взломами на уровне M2M-систем увеличились в два раза. Особенное внимание следует уделить области национальной безопасности.

проработанности вопроса реализации атак, направленных на компоненты ИТКС, реализующих межмашинное взаимодействие, можно сделать вывод о целесообразности проведения комплексных исследований в направлении оценки рисков реализации сетевых атак и управления защищенностью ИТКС, компоненты которых реализованы по технологии межмашинного взаимодействия.

Объектом исследования являются компоненты ИТКС, реализованные по технологии межмашинного взаимодействия, в отношении которых совершаются сетевые атаки.

Предметом исследования является оценка рисков реализации атак«IP-спуфинг»на ИТКС, компоненты которой реализованы по технологии межмашинного взаимодействия.

Цели и задачи исследования

Цель настоящей работы заключается в разработке методики оценки рисков реализации сетевых атак и управления защищенностью ИТКС, компоненты которой реализованы по технологии межмашинного взаимодействия. Для достижения указанной цели предполагается решить следующие задачи:

1. Построить описательную модель информационно-телекоммуникационной сети, как среды реализации сетевых атак, отражающую структуру сети и информацию, циркулирующую в M2M-сети, а также архитектуру современных сетей межмашинного взаимодействия для дальнейшей разработки математической модели реализации атак.

2. Провести анализ уязвимостей и угроз информационной безопасности информационно-телекоммуникационной сети, реализующей M2M-технологии с целью последующего выявления наиболее актуальной в рамках исследования атаки «IP-спуфинг».

3. Разработать математическую модельреализации атаки «IP-спуфинг»на M2M-компоненты с использованием сетей Петри-Маркова с целью исследования параметров M2M-сети, оказывающих влияние на размер ущерба и риска реализации атаки. Такая математическая модель должна отражать поэтапный процесс

реализации атаки IP-спуфинг и необходима для проведения риск-анализа и исследования защищенности информационно-телекоммуникационной сети.

4. Провести оценку функции ущерба реализации атаки «IP-спуфинг»на M2M-компонентыинформационно-телекоммуникационной сети путем анализа влияние параметровM2M-сети на размер ущерба реализации атаки с целью дальнейшего управления защищенностьюинформационно-телекоммуникационной сети.

5. Произвести оценку риска реализации атак с использованием «IP-спуфинг» и защищенности информационно-телекоммуникационной сети, компоненты которой реализованы по технологии межмашинного взаимодействия, позволяющую вывить наиболее уязвимые компоненты M2M-сети в рамках реализацииудаленной атаки «IP-спуфинг».

6. Разработать методику управлениефункцией защищенности,содержащую алгоритм управлениефункцией защищенности и отражающую влияние средств защиты и мероприятий по снижению рискав информационно-телекоммуникационной сети, компоненты которой реализованы по технологии межмашинного взаимодействия.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении к обозначенному предмету исследования.

В исследовании предполагается использовать методы теории вероятности, методы математической статистики и статистического анализа, методы теории графов, методы аналитического моделирования, методы теории рисков.

Научная новизна исследования

В настоящей работе получены следующие основные результаты, характеризующиеся научной новизной:

1. Разработанная описательная модель информационно-телекоммуникационной сети, которая отличается от известных тем, что включает