



Введение

8

1 Исследование технологий межмашинного взаимодействия

информационно-телекоммуникационной сети как объекта реализации

сетевых атак

14

1.1 Состав, строение и проблемы безопасности информационно-

телекоммуникационной сети в контексте применения технологий

межмашинного взаимодействия

14

1.1.1 Структура информационно-телекоммуникационной сети, реализующей

M2M-технологии

14

1.1.2 Информация, циркулирующая в M2M-сети

19

1.1.3 Политика безопасности информационно-телекоммуникационной сети,

реализующей M2M-технологии

23

1.1.4 Архитектура современных сетей межмашинного взаимодействия

25

1.2 Анализ уязвимостей и угроз информационной безопасности с

учетом реализации межмашинного взаимодействия компонент

информационно-телекоммуникационной сети

29

1.3 Требования информационной безопасности, предъявляемые к

технологиям межмашинного взаимодействия в современных

информационно-телекоммуникационной сети

35

1.4 Постановка задач исследования

38

2 Риск-моделирование атаки «IP-спуфинг» на информационно-

телекоммуникационные сети, компоненты которых реализованы по

технологии межмашинного взаимодействия

44

2.1 Действия злоумышленника и последствия реализации атаки «IP -

спуфинг» на информационно-телекоммуникационные сети,

компоненты которых реализованы по технологии межмашинного

взаимодействия

44

2.2	Разработка математической модели реализации удаленной атаки «IP-спуфинг» на информационно-телекоммуникационные сети, компоненты которых реализованы по технологии межмашинного взаимодействия	48
2.3	Оценка функции ущерба реализации атаки IP-спуфинг, направленной на получение конфиденциальной информации и вывод из строя оборудования предприятия	57
2.4	Оценка функции ущерба реализации удаленной атак «IP-спуфинг», направленной на замедление работы M2M-сети посредством вредоносных воздействий вируса	64
2.5	Обоснование выбора аналитического выражения функций риска и защищенности ИТКС, компоненты которых реализованы по технологии межмашинного взаимодействия	72
2.6	Основные выводы по главе	78
3	Оценка динамики изменения и управление функцией защищенности информационно-телекоммуникационной сети, компоненты которой реализованы по технологии межмашинного взаимодействия	79
3.1	Оценка динамики изменения функции защищенности M2M-сети в условиях реализации удаленной атаки «IP-спуфинг»	79
3.2	Расчет коэффициентов чувствительности защищенности информационно-телекоммуникационной сети, компоненты которой реализованы по технологии межмашинного взаимодействия	88
3.3	Управление функцией защищенности M2M-сети в условиях реализации удаленной атаки «IP-спуфинг»	96
3.4	Основные выводы по главе	102
	Заключение	103
	Список литературы	105



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 в 1989 году 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 в течение 2014 года увеличились в два раза. Особенное внимание следует уделить области национальной безопасности. В связи с тем, что одним из



важнейших направлений обеспечения информационной безопасности Российской Федерации является решение широкого круга вопросов, связанных с защитой информации при внедрении передовых информационных технологий в государственные системы связи и обработки информации, исследование по оценке рисков применения технологии межмашинного взаимодействия является важнейшей задачей[8,40].

Отсутствие полноценных и всесторонних работ, оценивающих деструктивные воздействия атак «IP-спуфинг» на компоненты технологии межмашинного взаимодействия ИТКС, наряду с широким применением таких технологий и ростом активности злоумышленников в области M2M-технологий, обуславливает необходимость проведения исследования с целью разработки методик оценки рисков и решения задач обеспечения безопасности и защиты информации в ИТКС, компоненты которой реализованы по технологии межмашинного взаимодействия. Необходимо тщательный анализ возможных угроз ИБ, ориентированных на M2M-компоненты, что позволит своевременно принять меры противодействия. В рамках данной работы будем рассматривать только преднамеренные угрозы нарушителей и злоумышленников. При анализе угроз необходимо оценить вероятность реализации атак «IP-спуфинг» на M2M-компоненты и сеть в целом, а также ущерб, который будет нанесен в случае не предотвращения угрозы с целью повышения уровня защищенности сети [5,6,19].

Степень проработанности темы

В настоящее время активно ведется изучение реализации различных сетевых атак «IP-спуфинг». Такие исследования можно встретить в различных работах, посвященных оценке рисков реализации атак в ИТКС [23,25,31,41,42,54,57].

Однако, несмотря на рост популярности M2M-технологии, существует мало работ, посвященных реализации сетевых атак на ИТКС, компоненты которой реализуют межмашинное взаимодействие, а исследования по оценке рисков реализации таких атак и защищенности ИТКС отсутствуют вовсе. [13, 35].

Таким образом, исходя из выявленного противоречия и степени научной

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 модель реализации 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-компоненты информационно-телекоммуникационной сети путем анализа влияния параметров M2M-сети на размер ущерба реализации атаки с целью дальнейшего управления защищенностью информационно-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 реализации удаленной атаки «IP-спуфинг».

6. Разработать методику управления функцией защищенности, содержащую алгоритм управления функцией защищенности и отражающую влияние средств защиты и мероприятий по снижению рисков 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



анализ угроз, связанных с работой M2M-технологии и учитывает архитектуру современных сетей межмашинного взаимодействия.

2. Разработанная модель ущерба реализации удаленной атаки «IP-спуфинг» отличается от известных тем, что в ней отражена структура сети межмашинного взаимодействия, позволившая исследовать действия злоумышленника применительно к M2M-технологии и оценить ущерб как на уровне единичного M2M-компонента, так и на уровне сети в целом.

3. Разработанный алгоритм управления функцией защищенности ИТКС, реализующей M2M-технологии, отличается от известных тем, что отражает степень влияния мероприятий по обеспечению работоспособности для компонентов, реализующих межмашинное взаимодействие.

Практическая ценность работы заключается в том, что:

1. Анализ угроз, воздействующих на M2M-компоненты информационно-телекоммуникационной сети, позволяет выявить наиболее опасные их виды и дает возможность владельцам ИТКС, реализующих M2M-технологии, уделить особое внимание защите от атак «IP-спуфинг».

2. Построенная модель ущерба реализации сетевых атак на компоненты, реализующие межмашинное взаимодействие, включает возможность дополнения необходимым набором параметров злоумышленника и информационно-телекоммуникационной сети. Такая модель позволяет владельцу определенной ИТКС оценить ущерб от реализации атаки «IP-спуфинг» конкретного злоумышленника, реализуя переход от универсальной к более точной модели.

3. Разработанные методические рекомендации внедрены в корпоративные и государственные информационно-телекоммуникационной сети с целью повышения защищенности сетей в отношении противодействия удаленным атакам «IP-спуфинг» на компоненты, реализующие межмашинное взаимодействие.



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT