Аннотация – В этом документе представлен анализ воздействия кибер-атак на деятельность морских портов с акцентом на количественную оценку эконометрических потерь. В ходе анализа рассмотрены различные аспекты, включая прямые понесённые экономические потери, эффекты для различных секторов промышленности, конкретные уязвимости и последствия кибер-атак, а также меры безопасности в морских портах. Анализ полезен специалистам в области безопасности, ИТ-экспертам, и заинтересованным сторонам из различных отраслей, поскольку даёт представление о масштабах потенциальных сбоев и позволяет вести разработку надёжных стратегий для противодействия кибер-проблемам. Выводы, полученные в результате анализа, имеют значение для повышения готовности к кибер-угрозам в критически важной национальной инфраструктуре и реагирования на них, обеспечивая тем самым экономическую стабильность и национальную безопасность.

I. Введение

В документе «Quantifying the econometric loss of a cyber-physical attack on a seaport» представлено всестороннее исследование экономических последствий кибер-атак на морскую инфраструктуру, которые являются важнейшими компонентами глобальной торговли и цепочек поставок и вносят значительный вклад в понимание уязвимости и экономических последствий кибер-угроз в секторе.

Суть исследования заключается в разработке и применении эконометрической модели (EC), предназначенной для количественной оценки экономических потерь в результате кибер-атак на морские порты. Кибер-эконометрическая модель (CyPEM), представляет собой структуру из пяти частей, объединяющая различные аспекты кибер-систем, анализ экономического воздействия и стратегии управления рисками. Методология включает системный подход к моделированию начальных экономических последствий кибер-атаки, которая, хотя и начинается локально, может иметь далеко идущие глобальные последствия из-за взаимосвязанного характера глобальной торговли и цепочек поставок.

Полученные результаты подчёркивают значительную экономическую уязвимость морских портов к кибер-атакам. За счёт применения в CyPEM, исследователи смогли определить количество потенциальных эконометрических убытков, оказывающие влияние не только на целевой порт, но и более широко на глобальную морскую экосистему и цепочек поставок. Результаты модели подчёркивают каскадные последствия сбоев в работе морских портов, которые могут привести к значительным экономическим потерям как на местном, так и на глобальном уровне. Это служит конкретным примером того, как модель может быть использована для оценки экономических последствий кибер-атак на морские порты.

В документе также подчёркивается конвергенция ИТ и операционных технологий как преобразующей силы в морском секторе, создающей цифровые маршруты поставок и модернизирующей морские операции. Однако это «сближение» также расширяет зону кибер-угроз, делая критически важную морскую инфраструктуру более восприимчивой к кибератакам. Угроза исходит не только от обычных киберпреступников, но и от субъектов национальных государств и организованных преступных групп, обладающих ресурсами и мотивацией для нанесения ударов по критической национальной инфраструктуре.

A. Преимущества предлагаемого решения:

- Возможность количественной оценки потенциального экономического воздействия кибер-атаки на морской порт локально и глобально
- Помогает выявлять потенциальные уязвимости и слабые места в цепочке поставок, позволяя лучше готовиться к кибератаками реагировать на них
- Адаптация для анализа различных кибер-систем

B. Недостатки предлагаемого решения:

- Небольшой размер выборки опроса, используемого для оценки общественного восприятия кибер-рисков на морском транспорте
- Для эффективного использования могут потребоваться профильные знания и опыт
- Сложность модели может затруднить понимание и использование результатов некоторыми заинтересованными сторонами
- Не учитывает другие потенциальные последствия кибер-атак, такие как воздействие на окружающую среду или безопасность.

C. Применение

Предлагаемая структура полезна для количественной оценки эконометрических потерь в результате кибер-события. Эконометрические результаты кибер-атаки на порт позволили сравнить фактический риск для кибербезопасности с воспринимаемым общественностью риском, связанным с морскими кибер-угрозами, и то, как это влияет на них.

Применение инструмента заинтересованными сторонами возможно для лучшей количественной оценки и

понимания их конкретных кибер-рисков, включая связанные со страхованием корпорации, которые на региональном и / или глобальном уровнях подвержены рискам, связанным с непредвиденными перерывами в работе, и организации, производственная деятельность которых связана с глобальными цепочками поставок. Возможность обмена отдельными этапами фреймворка также позволяет моделировать другие сектора, помимо морского, и морские сценарии, а также учитывать кибер-сбои на разных узлах.

Правительственные организации, портовые администрации, субъекты грузовых перевозок и логистики, а также торговые ассоциации также могут быть заинтересованы в предлагаемой системе, поскольку она может помочь лучше понять их ландшафт рисков и выявить конкретные слабые места или зависимости, которые, если их использовать, могут оказать значительное влияние на национальную экономику.

II. Морская кибербезопасность

Морская кибербезопасность становится все более важной областью, вызывающей озабоченность в отрасли, поскольку новые технологии, такие как Интернет вещей (IoT), цифровые двойники, 5G и искусственный интеллект (ИИ), становятся все более распространёнными в этом секторе. Конвергенция и цифровизация информационных технологий (ИТ) и операционных технологий (ОТ) привели к трансформации цифровых маршрутов поставок и морских операций, расширив масштабы кибер-угроз.

Интеграция цифровых технологий в критически важные операции в морском секторе создаёт значительные кибер-уязвимости, которые могут привести к более масштабным глобальным сбоям. По мере ускорения перехода сектора к цифровизации крайне важно понимать и количественно оценивать потенциальные последствия кибер-сбоев.

A. Ключевые моменты

- Возросшие масштабы судоходства и размеров судов (крупные суда большей вместимости) привели к проблемам с маневрированием в существующих каналах и морских портах, снижая запас прочности во время кибер-инцидентов. Современные корабли также оснащены более мощным оборудованием, что увеличивает степень угрозы кибератак.
- Береговая охрана США сообщила об увеличении числа морских кибер-инцидентов на 68%, а недавние исследования показывают, что кибер-риски в морской пехоте и морских технологиях присутствуют и растут по мере внедрения новых решений.
- Хотя цифровизация в сфере судоходства обеспечивает повышение производительности, физическую безопасность, снижение выбросов углекислого газа, более высокую эффективность, более низкие затраты и гибкость, в крупных сенсорных сетях CPS и системах связи существуют уязвимые места.
- Опрос показал, что 64% респондентов считают, что порт уже испытал значительный физический ущерб, вызванный кибер-инцидентом, а 56% считают, что торговое судно уже испытало значительный физический ущерб, вызванный инцидентом кибербезопасности.

B. Второстепенные моменты

- **Новые технологии**: Морской сектор внедряет новые технологии в офисах, на судах, в морских портах, оффшорных сооружениях и многом другом. Эти технологии включают Интернет вещей (IoT), цифровых двойников, 5G и искусственный интеллект (AI).
- **Цифровизация цепочки поставок**: Цепочки поставок также используют все больше информационных технологий (ИТ), создавая цифровые уязвимости. Конвергенция ИТ и операционных технологий (ОТ) трансформирует цифровые маршруты поставок и морские операции, расширяя возможности противодействия кибер-угрозам.
- **Кибер-угрозы**: субъекты национальных государств и организованная преступность обладают ресурсами и мотивацией для запуска кибератаки на критическую национальную инфраструктуру (CNI), такую как крупномасштабные кибер-системы, которые включают морские операции.
- **Кибер-системы**: Интеграция физических процессов с программным обеспечением и сетями связи, известными как кибер-системы, является важной частью цифровой трансформации морского сектора. Однако это также создаёт новые проблемы в области кибербезопасности.
- **Последствия кибератак**: атаки на инфраструктуру имеют значительные экономические последствия, затрагивая не только целевой морской порт, но и более широкую глобальную морскую экосистему и цепочки поставок.

III. Кибер-угроза

Морской сектор становится все более уязвимым к угрозам кибербезопасности, которые могут иметь далеко идущие последствия для других областей из-за взаимосвязанного характера современных перевозок. По мере дальнейшего развития технологий растёт вероятность разрушительных событий, вызванных злонамеренными кибератаками, о чем свидетельствуют недавние отчёты и академические исследования. Чтобы понять потенциальный масштаб этих сбоев, важно изучить влияние крупных сбоев в цепочке поставок на цель атаки и остальную часть связанной с ней цепочки поставок. Эти события привели к многочисленным бизнеса, причём большинство исков поступило из районов, находящихся за пределами непосредственно затронутых регионов.

Текущие возможности киберзащиты вряд ли позволят предотвратить все кибер-катастрофы, что делает крайне важным количественную оценку и понимание последствий таких событий. Основное внимание уделяется взаимозависимостям в современных глобальных цепочках поставок и представлена эконометрическая модель (EM), которая позволяет организациям перейти от качественной

оценки к более надёжной количественной оценке рисков цепочки поставок.

Мировые производственные сети снабжения подвержены нарушениям в результате кибератак, которые могут распространяться по сети и оказывать негативное физическое и экономическое воздействие на соседние, предшествующие и последующие узлы. Кибератаки с использованием сетей IT / OT и вычислительных систем могут привести к краткосрочным потерям, отказу в обслуживании (DoS), долгосрочному выводу из строя оборудования, потере доверия клиентов, задержкам в отправке и потере стратегических преимуществ из-за утечек и компрометации конфиденциальной информации. Цифровые кибератаки также могут иметь реальные физические последствия, такие как невыполненный спрос на транспортировку товаров и производство.

A. *Ключевые points*

- С увеличением темпов технологического роста возрастает вероятность событий, вызванных злонамеренными кибератаками в секторе.
- Экономические и страховые убытки, возникающие в результате сбоев в цепочке поставок, являются одними из основных возникающих рисков для глобальных корпораций и страховщиков.
- Поскольку нынешние возможности киберзащиты вряд ли позволят предотвратить все кибер-катастрофы, крайне важно количественно оценить и понять последствия таких событий.
- В исследовании основное внимание уделяется тому, как крупные сбои в цепочке поставок влияют на цель атаки и остальную связанную с ней цепочку поставок, представленную в классическом формате графов с "узлами", представляющими активы, и "рёбрами", соединяющими узлы.
- Эконометрическая модель (EM) позволяет организациям перейти от качественной оценки рисков цепочки поставок к более надёжной количественной оценке.
- Интегрируя EM с динамической моделью кибер-рисков MaCRA, объединённая модель позволяет пользователю получать количественные данные о смоделированных потерях для улучшения понимания кибер-рисков глобальной цепочки поставок, что приводит к повышению кибер-устойчивости и надёжности системы.

B. *Реалистичное моделирование*

- Тематическое исследование было проведено на базе европейского морского порта в Испании и классе контейнеровозов, которые обычно заходят в тот же порт. И порт, и судно моделируются на основе реальных данных путём цифровизации физических характеристик в цифровые.
- Порт Валенсии генерирует почти 51% ВВП Испании и является важным игроком в европейских и глобальных цепочках поставок, соединяющих Азию и Америку. Любой сбой в работе этого порта приведёт к прямым экономическим потерям для Испании и отразится на различных физических узлах и цепочках создания стоимости.
- Известные решения по управлению рисками в цепочке поставок (SCRM) содержат многочисленные основы и модели для определения типов и источников рисков, а также стратегий смягчения последствий, но без адаптации к «технологическому ландшафту Индустрии 4.0».
- Эконометрическая модель (EM) с использованием полностью количественной модели с полным отображением узловой сети для точного представления сквозного жизненного цикла продукта и расчёта эконометрического воздействия существующей сети цепочки поставок.
- Сбои в кибер-системе (CPS) распространяются между физическими уровнями и кибер-уровнем из-за высоких взаимосвязей и взаимозависимости. Факторы риска варьируются от физических до кибернетических, от статических до динамических.

IV. Фреймворк

Применяется «гибридный» метод моделирования, который использует частично отображённые цепочки поставок и использует прогнозную аналитику для заполнения недостающих частей. Такой подход позволяет избежать недооценки риска за счёт выявления скрытых уязвимостей и корреляций, проистекающих из невидимых или неизвестных звеньев данной цепочки поставок. Модель риска цепочки поставок является первой в своём роде, поскольку это количественная модель, которая включает глобальные модели торговли и сетей поставок, отображение товарных потоков и корреляцию между различными товарными группами и отраслями.

CyPEM даёт организациям возможность провести стресс-тестирование устойчивости цепочек поставок путём оценки затрат и времени на восстановление после различных сценариев кибератак. Система включает количественные модели рисков, которые имитируют основные компоненты глобальных цепочек поставок и их неопределённости для оценки временных задержек и экономических потерь в результате условного прерывания бизнеса (CBI). Время простоя измеряется количеством дней или часов, вызванных кибер-сбоями в работе данного узла цепочки поставок.

Фреймворк разработан для обеспечения определённой динамической автоматизации при расчёте кибер-эконометрических потерь. Некоторые переменные сценария кибератаки могут быть изменены «в реальном времени» на различных этапах для изучения ряда эконометрических результатов. Этот инструмент позволяет пользователям активно управлять рисками в цепочке поставок, предвидя корреляции в цепочках поставок, а также последствия разрушительных событий, вызванных киберпространством, до того, как они могут произойти. Количественные результаты также важны для измерения различий между предполагаемым и реальным риском в понимании экспертов и непрофессионалов.

Фреймворк предназначен для предоставления аналитики по различным звеньям или секторам цепочки

поставок и может использоваться для информирования о поддающихся количественной оценке кибер-рисках.

- **Определение отрасли, промежуточных частей и конечных продуктов**: определение отрасли, промежуточных частей и конечных продуктов анализируемой цепочки поставок.
- **Определение сети, в которой узлы являются поставщиками, а ребра - потоками продукции / деталей**: на этом этапе определяется сеть цепочки поставок, где узлы представляют поставщиков, а ребра - потоки продукции или деталей.
- **Расчёт сбоев с использованием оценки кибер-рисков и модели пропускной способности порта**: расчёт сбоев с использованием модели оценки рисков и пропускной способности порта.
- **Расширение на остальную часть сети**: на этом этапе учитывается распространение сбоя дальше по сети цепочки поставок для оценки воздействия на другие узлы и границы.
- **Расчёт отраслевых убытков**: расчёт отраслевых убытков и их распределения в результате сбоя.

Первые два этапа включают создание ациклических сетевых графиков с использованием статистики торговли сырьевыми товарами и товарных потоков стран для установления зависимостей по продуктам. После установления зависимости от продукта торговые данные из статистики торговли сырьевыми товарами используются для создания сети, включающей узлы хранения и транспортировки, а также цепочки поставок компонентов на основе межотраслевых зависимостей.

Следующим этапом разработки структуры является определение сети, которое выходит за рамки продуктовых зависимостей и учитывает производство и транспортировку в стране для определения товарных потоков. В то время как модель в настоящее время использует ациклическую сеть для представления потока продуктов без создания циклов обратной связи, будущее моделирование на этом этапе может быть заменено на другой тип сети в зависимости от конечного использования всей структуры. Данные, используемые для определения и создания будущих сетей, могут включать период данных, поток (т. е. импорт / экспорт), коды товаров, торговую стоимость, вес нетто, количество и статистику.

Предлагаемая сеть является гибридной, которая объединяет график зависимости продукта (или дерево) с первого этапа и соответствующие торговые данные со второго этапа. Этот шаг гарантирует, что эконометрическая модель сможет учитывать динамику торговли между странами и отраслевыми границами в рамках товарных категорий. Результирующая гибридная сеть является ключом к определению эконометрических потерь от кибер-сбоя на более поздних этапах CyPEM.

Прогнозная аналитика может улучшить графики зависимостей продукта на ранних этапах, точность и детализация которых зависят от последующих этапов. CyPEM собирает данные из многочисленных источников и устаревших систем, чтобы получить полное представление о цепочке поставок, а последующий анализ проводится для выявления полезной информации и повышения уровня интеллектуальных данных. Аналитика используется для автоматизации принятия сложных решений и упреждающего и динамического обновления рекомендаций на основе изменяющихся событий, чтобы воспользоваться преимуществами этих прогнозов и повысить ценность инструментов классификации проектов. Применение этих сетей для предварительного определения атрибутов рынка и зависимостей, а также того, как они влияют на остальную часть сети, сохраняя при этом фактические события сбоев (и все их отдельные элементы) более динамичными.

Структура CyPEM предполагает расчёт сбоев с использованием двух моделей: модели оценки морских кибер-рисков и кибер-модели пропускной способности порта. Модель оценки морских кибер-рисков использует цепочку кибер-атак, чтобы показать ряд потенциальных рисков и результатов, в зависимости от успеха каждого сегмента цепочки атак. Цепочка атак, используемая в этой модели, была подтверждена фактическими данными и экспериментами на испытательном стенде, которые были сопоставлены с уязвимостями системы на судах, которые, как известно, заходят в порт в 2021 и 2022.

Вторая часть расчёта сбоев заключается в учёте кибер-рисков и их последствий, а также в прогнозировании общего эффекта сбоев в работе портов. Для этого была разработана кибер-модель пропускной способности порта. Этот процесс похож на первые два этапа, но используется одного порта, а не всей глобальной сети. Предлагаемый метод позволяет сделать модель более детализированной, моделируя даже отдельные суда и терминальные краны (включая их тип), чтобы точно определять время простоя порта в часах, а также в процентах.

Чтобы модель пропускной способности имитировала портовые операции, необходимо учитывать определённые параметры, описывающие трафик и потоки внутри порта:

- процесс прибытия,
- количество контейнеров за один заход в порт,
- распределение времени обслуживания на судно,
- долю контейнеров, предназначенных для перегрузки,
- среднее время пребывания контейнеров в порту.

Наблюдается, что сбой, вызванный кибератакой, снижает производственные / транспортные возможности узлов и оказывает волновой эффект на последующие узлы. Если циклические цепочки поставок будут интегрированы в систему в качестве следующего шага в будущем, характер сбоев и результаты могут сильно отличаться. Глобальная кибератака может отличаться от других стихийных бедствий, которые могут быть локализованы географически, в то время как кибератаки, как правило, происходят там, где расположены целевые системы. Следовательно, одна цифровая угроза может спровоцировать кибер-инциденты в нескольких географических регионах или охватить несколько секторов (например, здравоохранение, производство), если используется аналогичная базовая технология.