Аннотация – быстро и незаметно для мирового сообщества, особенно для той части, которая движет фундаментальную науку вперёд, США приостановили свои научные исследования в невероятно значимом регионе Антарктике. Да, как на колоссальном и почти неисследованном континенте, так и в окружающих морских водах. Причина? Об этом можно догадаться с одной попытки, поскольку это стало обычным явлением для всего мира: нехватка средств. С другой стороны, существует острая необходимость в управлении конкретными кибер-угрозами в Антарктике…

I. Введение

В апреле Национальный научный фонд США (NSF) объявил, что не будет поддерживать какие-либо новые полевые исследования в этом сезоне из-за задержек с модернизацией станции Макмердо. Национальный фонд и береговая охрана США также объявили о сокращениях, которые поставят под угрозу научные и геополитические интересы США в регионе на десятилетия вперёд. В частности, в апреле NSF объявил, что не будет продлевать аренду одного из двух своих антарктических исследовательских судов "Laurence M. Gould". До этого, в октябре 2023 года, NSF объявил, что в ближайшие десятилетия будет эксплуатировать только одно исследовательское судно.

Кроме того, в марте Береговая охрана США объявила, что ей необходимо "пересмотреть базовые показатели" для своей давно отложенной программы Polar Security Cutter, жизненно важной для национальных интересов США на обоих полюсах. Принятые решения, будут иметь серьёзные последствия для деятельности США в Антарктике даже за 2050 годом.

Государственный департамент воздержался от объявления внешнеполитических интересов США в Антарктическом регионе, и Белый дом, похоже, удовлетворён устаревшей и непоследовательной национальной стратегией в отношении Антарктики прошлого века. Конгресс США также не ответил на призывы учёных.

В результате 1 апреля Управление полярных программ NSF объявило, что оно приостанавливает новые предложения по полевым работам на следующие два сезона и не будет запрашивать их в Антарктиде.

Суда, способные работать в полярных морях, становятся все более востребованными, но строить их все труднее. Столкнувшись со значительными проблемами в проекте строительства кораблей и катеров ледового класса, Береговая охрана США объявила в марте, что она "сдвинет базовые сроки" разработки новых проектов ледоколов.

Результатом этих, казалось бы, независимых решений станет сокращение физического присутствия США в Антарктиде. Это будет иметь негативные последствия не только для американских учёных, но и для геополитики США в регионе, особенно учитывая тотальное превосходство России в ледоколах и догоняющее влияние Китая.

США упустили из виду наиболее важные аспекты: адекватное и регулярное финансирование научных исследований в Антарктике, новую национальную стратегию (текущая стратегия была опубликована в июне 1994 года) и понимание законодателями важности интересов и решений США в Антарктике. Неспособность финансировать оперативную и материально-техническую поддержку, необходимую для научных исследований и геополитического влияния США, эффективно означает доминирование России и Китая в антарктическом регионе, поскольку никакая другая страна, включая традиционных участников, таких как Чили, Австралия и Швеция, не может превзойти существующий и растущий научный потенциал России и Китая.

A. Ключевые аспекты

- **США сокращает исследовательские операции в Антарктике**: США объявили о значительном сокращении своих исследовательских операций в Антарктике из-за проблем с финансированием и задержек с модернизацией критически важной инфраструктуры, такой как станция Мак-Мердо. Это включает в себя отказ от продления аренды исследовательского судна Laurence M. Gould и эксплуатацию только одного исследовательского судна в ближайшие десятилетия.
- **Проблемы в программе ледоколов США**: береговая охрана США объявила о задержках в своей программе катеров Polar Security, которая имеет решающее значение для поддержания присутствия и операций США в полярных регионах. Переоценка этой программы указывает на значительные проблемы и потенциальные долгосрочные последствия для возможностей США в Антарктике.
- **Геополитические последствия вывода войск США**: сокращение присутствия США в Антарктике имеет более широкие геополитические последствия,

особенно по мере того, как Россия и Китай продолжают расширять свои возможности и влияние в регионе. Отсутствие современной национальной стратегии и адекватного финансирования антарктических операций ставит США в невыгодное положение.

- **Влияние на научные исследования**: приостановление новых предложений NSF о проведении полевых работ повлияет на научные исследования в Антарктиде, задерживая важные исследования и потенциально приводя к потере ценных данных. Это решение выдвигает на первый план более широкую проблему финансирования и поддержки научных начинаний в отдалённых регионах.

II. Влияние

Решение США приостановить научные исследования в Антарктиде вызвало различные реакции со стороны других стран, особенно тех, у которых есть значительные интересы и операции в регионе. Это решение, обусловленное бюджетными ограничениями и задержками в модернизации критически важной инфраструктуры, имеет не только геополитические последствия.

A. Геополитические последствия

1) Снижение влияния США:

- Сокращение присутствия США придаст смелости другим странам преследовать свои индивидуальные интересы в Антарктике.

2) Активизация действий соперничающих держав

- **Китай**: Китай расширяет своё присутствие в Антарктиде, и отступление США ускорит эту тенденцию. Китай недавно открыл свою пятую исследовательскую станцию в Антарктиде и наращивает научный и логистический потенциал в регионе. Расширение деятельности Китая вызывает обеспокоенность по поводу потенциальных технологий двойного назначения, которые могут служить как научным, так и военным целям. Растущее влияние Китая в Антарктиде может изменить баланс сил и усилить геополитическую напряжённость.

- **Россия**: Россия также наращивает свою деятельность в Антарктике, включая создание новых исследовательских станций. Прогресс России в области ледокольных технологий и её стратегическое позиционирование в регионе будут подкреплены сокращением присутствия США. Это приведёт к усилению доминирующей роли России в управлении Антарктидой и научных исследованиях, что ещё больше бросит вызов интересам США.

3) Реакция партнёров

- **Австралия**: Австралия, ключевой игрок в делах Антарктики, выразила обеспокоенность по поводу решения США. Австралия активно участвует в исследованиях и управлении Антарктикой и полагается на международное сотрудничество для достижения своих научных и экологических целей. Отступление США может побудить Австралию увеличить собственные инвестиции в исследования и укрепить партнёрские отношения с другими странами, чтобы «заполнить пустоту», оставленную США

- **Великобритания**: Великобритания также внесла значительный вклад в исследования в Антарктике. Страна стремится расширить своё научное присутствие и сотрудничество с другими странами для обеспечения дальнейшего прогресса в исследованиях. Правительство Великобритании подчеркнуло важность сохранения сильного международного присутствия в Антарктике для решения глобальных экологических проблем и соблюдения принципов системы Договора.

4) Стратегические уязвимости:

- Решение США сократить свои операции может выявить стратегическую уязвимость, особенно по мере того, как новые технологии снижают барьеры для стран, стремящихся увеличить своё присутствие и извлечь выгоду из ресурсов региона. Это также включает в себя потенциал для военного применения, такого как разведка и спутниковое позиционирование

- Отсутствие надёжного присутствия США может привести к стратегическому дисбалансу, когда Россия и Китай потенциально будут доминировать в регионе. Это может иметь долгосрочные последствия для глобальной безопасности и национальных интересов США.

B. Научные и экологические последствия

1) Влияние на научные исследования:

- Приостановление новых предложений NSF о проведении полевых работ приведёт к задержке важных научных исследований, к пробелам в знаниях, которые имеют решающее значение для понимания глобальных изменений окружающей среды (исследования по изменению климата, повышению уровня моря и закономерностям океанической циркуляции).

- Сокращение научной деятельности США может помешать международному научному сотрудничеству, поскольку многие страны полагаются на её инфраструктуру и материально-техническую поддержку в своих исследованиях в Антарктиде

2) Экологические риски:

Сокращение присутствия США может повлиять на мониторинг окружающей среды и усилия по её сохранению. Регион Антарктики имеет решающее значение для изучения изменения климата и его воздействия на глобальные экосистемы. Сокращение исследовательской деятельности может замедлить прогресс в этих областях и снизить эффективность мер по охране окружающей среды.

Больше материалов: Boosty | Sponsr | TG

Экологические проблемы также имеют первостепенное значение. Антарктида является критически важным регионом для изучения изменения климата и его воздействия на глобальные экосистемы. Приостановка научных исследований в США может замедлить прогресс в понимании этих последствий и смягчении их. Другим странам, возможно, потребуется активизировать свои исследовательские усилия, чтобы компенсировать сокращение вклада США, гарантируя продолжение сбора и анализа важнейших экологических данных

3) Национальная безопасность:

Решение США сократить своё присутствие в Антарктиде может иметь последствия для национальной безопасности, особенно если конкурирующие державы будут использовать регион в военных целях. Стратегическое расположение Антарктиды делает её потенциальным местом для разведки и другой военной деятельности, которая может угрожать глобальной безопасности

III. Кибер-атаки

Морская отрасль в Антарктиде сталкивается с целым рядом кибер-угроз, включая фишинг, вредоносное ПО, несанкционированный доступ, подмену GPS, атаки на цепочки поставок и атаки на операционные технологии. Угрозы усугубляются суровыми экологическими условиями региона и растущей зависимостью от цифровых систем.

A. Фишинговые атаки

- **Описание**: атаки связаны с ложными электронными письмами и сообщениями, предназначенными для обмана морского персонала с целью раскрытия конфиденциальной информации или загрузки вредоносного ПО. Фишинговые атаки могут привести к несанкционированному доступу к системам судна и конфиденциальным данным.
- **Влияние**: фишинг ставит под угрозу навигационные системы, сети связи и операционные технологии, потенциально приводя к значительным сбоям в работе.

B. Вредоносное ПО и программы-вымогатели

- **Описание**: вредоносное программное обеспечение может использоваться для нарушения работы встроенных систем, кражи конфиденциальных данных или блокировки законных пользователей, часто требуя выкуп за восстановление доступа.
- **Воздействие**: атаки вредоносных программ и программ-вымогателей могут вывести из строя критически важные системы, что приведёт к задержкам в работе и финансовым потерям. Эти атаки вызывают особую озабоченность, учитывая зависимость Антарктиды от цифровых систем навигации и связи.

C. Несанкционированный доступ и внутренние угрозы

- **Описание**: несанкционированный доступ предполагает получение доступа к системам без разрешения, часто путём использования уязвимостей или украденных учётных данных. Внутренние угрозы связаны с сотрудниками или подрядчиками, которые намеренно или непреднамеренно ставят под угрозу безопасность.
- **Влияние**: несанкционированный доступ и угрозы со стороны инсайдеров могут привести к утечке данных, сбоям в работе системы и потере конфиденциальной информации. Эти угрозы сложно обнаружить и смягчить, особенно в изолированных средах, таких как Антарктида.

D. Подмена GPS

- **Описание**: злоумышленники манипулируют сигналами GPS, чтобы ввести морские навигационные системы в заблуждение относительно местоположения или маршрута судна.
- **Влияние**: подмена GPS приведёт к ошибкам навигации, несанкционированным объездам и потенциальным авариям. Это особенно опасно в сложных условиях вод вокруг Антарктиды, где точная навигация имеет решающее значение.

E. Атаки на цепочки поставок

- **Описание**: атаки нацелены на взаимосвязанные системы и сети морской цепочки поставок, включая порты, поставщиков логистических услуг и другие сторонние сервисы.
- **Воздействие**: атаки на цепочку поставок могут нарушить всю морскую операцию, что приведёт к задержкам, финансовым потерям и поставит под угрозу безопасность груза и персонала.

F. Кибер-атаки на операционные технологии (OT)

- **Описание**: системы OT, которые включают промышленные системы управления (ICS), используемые для навигации, управления двигателем и обработки грузов, все чаще становятся мишенями хакеров.
- **Воздействие**: атаки на системы OT нарушают критически важные операции, что приводит к угрозам безопасности, задержкам в работе и значительным финансовым потерям. Интеграция IT- и OT-систем в морской отрасли увеличила поверхность атаки, сделав эти системы более уязвимыми.

IV. Проблема кибербезопасности

Морская отрасль Антарктиды сталкивается с уникальными проблемами кибербезопасности, которые обусловлены удалённостью и суровыми условиями окружающей среды, интеграцией устаревших и современных систем, неопределённостью нормативных актов и нехваткой квалифицированных специалистов.

Больше материалов: Boosty | Sponsr | TG

A. Суровые условия окружающей среды

- **Экстремальные погодные условия**: суровые и непредсказуемые погодные условия в Антарктиде могут нарушить работу систем связи и электроснабжения, что затруднит поддержание последовательных мер кибербезопасности.
- **Изоляция**: удалённый и изолированный характер операций в Антарктике означает, что физический доступ к инфраструктуре для технического обслуживания и реагирования на инциденты ограничен, что усложняет усилия по обеспечению кибербезопасности.

B. Интеграция IT- и OT-систем

- **Комплексная интеграция**: морская отрасль, включая операции в Антарктике, все больше полагается на интеграцию систем информационных технологий (ИТ) и операционных технологий (ОТ). Такая интеграция создаёт сложные проблемы кибербезопасности, поскольку эти системы традиционно были отдельными, а теперь взаимосвязаны, увеличивая поверхность атаки.
- **Устаревшие системы**: во многих морских операциях по-прежнему используются устаревшие системы, которые не были разработаны с учётом кибербезопасности. Эти системы теперь подключены к современным сетям, создавая уязвимости, которыми могут воспользоваться кибер-атаки.

C. Вопросы регулирования и соблюдения требований

- **Неоднозначность регулирования**: морская отрасль сталкивается с неоднозначностью регулирования, особенно в отдалённых регионах. Существующие нормативные акты, такие как Кодекс международной безопасности судов и портовых средств (ISPS) и Закон о безопасности морского транспорта (MTSA), были разработаны в доцифровую эпоху и могут не в полной мере отражать текущие кибер-угрозы.
- **Международное сотрудничество**: учитывая глобальный характер морских операций, международное сотрудничество имеет важное значение для установления единых стандартов и протоколов кибербезопасности. Это особенно сложно в Антарктиде, где интересы и операции имеют несколько стран.

D. Технологические достижения и угрозы

- **Расширение возможностей подключения**: внедрение облачных вычислений, Интернета вещей (IoT) и автономных технологий в морских операциях привело к усилению взаимосвязи между ИТ-системами и системами ОТ. Такое подключение повышает риски кибербезопасности, о чем свидетельствует увеличение кибер-атак на морские системы ОТ на 900% за последние три года.
- **Возникающие угрозы**: морская отрасль является главной мишенью для кибер-угроз, включая злоумышленников со стороны национальных государств и киберпреступников, стремящихся сорвать операции, украсть данные или потребовать выкуп. Меняющийся ландшафт угроз требует постоянного мониторинга и обновления мер кибербезопасности.

E. Рабочая сила и опыт

- **Нехватка специалистов по кибербезопасности**: в морской отрасли наблюдается повсеместная нехватка квалифицированных специалистов по кибербезопасности. Этот дефицит усугубляется в отдалённых регионах где привлечение и удержание талантов является особенно сложной задачей.
- **Обучение и осведомлённость**: программы непрерывного обучения и осведомлённости необходимы для поддержания высокого уровня готовности к кибербезопасности. Однако логистические проблемы, связанные с проведением таких программ в Антарктике, могут снизить их эффективность.

F. Реагирование на инциденты и восстановление

- **Ограниченные возможности реагирования на инциденты**: способность реагировать на кибер-инциденты и восстанавливаться после них ограничена в Антарктиде из-за изоляции региона и суровых условий. Это делает крайне важным наличие надёжных возможностей удалённого мониторинга и реагирования на инциденты.
- **Отчётность о кибер-инцидентах**: недавнее распоряжение администрации Байдена-Харриса подчёркивает необходимость отчётности о кибер-инцидентах. Однако реализация этих требований в Антарктике может оказаться сложной задачей из-за ограничений в области связи и различий в нормативных актах.

V. Особые меры кибербезопасности

Морская отрасль в Антарктике может эффективно противостоять угрозам кибербезопасности, внедряя целостную систему кибербезопасности, соблюдая нормативные стандарты, используя передовые технологические решения, обеспечивая всестороннее обучение, разрабатывая надёжные планы реагирования на инциденты и укрепляя международное сотрудничество.

A. Целостная система кибербезопасности

- **Интеграция информационных технологий и безопасности ОТ**: конвергенция систем информационных технологий (ИТ) и операционных технологий (ОТ) в морской отрасли требует целостного подхода к кибербезопасности. Использование таких платформ, как NIST Cybersecurity Framework и ISA/IEC IACS Cybersecurity Lifecycle Model, помогает в оценке,

планировании, внедрении и мониторинге мер кибербезопасности как в ИТ, так и в ОТ-средах.

- **Комплексное управление рисками**: разработка и внедрение широкого спектра средств контроля корпоративной кибербезопасности, охватывающих как суда, так и береговые объекты, имеет важное значение. Это включает в себя обращение к системам IT, OT и интернета вещей для обеспечения безопасной критической морской инфраструктуры.

B. Соответствие нормативным требованиям и стандартам

- **Соблюдение Руководящих принципов ИМО**: международная морская организация (IMO) выпустила принципы по управлению кибер-рисками на море, которые содержат рекомендации высокого уровня и функциональные элементы для минимизации рисков и воздействия на операции, связанные с судоходством, охрану и охраняемость.
- **Соблюдение CAP и UNCLOS**: CAP и Конвенция UNCLOS обеспечивают правовую основу для морских операций в Антарктике. Обеспечение соблюдения этих правил, включая требования к регистрации судов и оборудованию для обеспечения безопасности, имеет решающее значение для поддержания безопасности на море.

C. Передовые технологические решения

- **Сегментация сети**: Разделение сети на отдельные сегменты помогает сдерживать потенциальные взломы и затрудняет боковые перемещения для злоумышленников. Это особенно важно для защиты критически важных систем на судах и в портовых сооружениях.
- **Регулярное тестирование на проникновение**: Проведение регулярных тестов на проникновение для выявления и устранения уязвимостей, прежде чем они смогут быть использованы злоумышленниками, является упреждающей мерой повышения кибербезопасности.
- **Искусственный интеллект и машинное обучение**: Внедрение передовых систем обнаружения угроз, которые используют искусственный интеллект и машинное обучение для обнаружения необычного поведения, может помочь выявлять и смягчать кибер-угрозы в режиме реального времени.
- **Передовые системы кибербезопасности**: Использование передовых систем кибербезопасности, таких как Cydome's Everlight, поддерживает управление кибербезопасностью судна посредством мониторинга и оценки рисков в режиме реального времени. Эти системы помогают эффективно обнаруживать и смягчать кибер-угрозы

D. Обучение и осведомлённость

- **Учебные программы по кибербезопасности**: важно обеспечить всестороннюю подготовку по кибербезопасности всего персонала, как моряков, так и берегового персонала. Учебные программы должны охватывать новейшие угрозы безопасности, тактику фишинга и лучшие практики предотвращения кибер-атак.
- **Обучение и осведомлённость пользователей**: Регулярное информирование сотрудников о передовых методах кибербезопасности и новейших угрозах гарантирует, что они будут лучше подготовлены к обнаружению и предотвращению кибер-атак, снижая риск человеческой ошибки.

E. Реагирование на инциденты и восстановление

- **План реагирования на инциденты**: Разработка и регулярное обновление плана реагирования на инциденты обеспечивает быстрые действия и смягчение последствий в случае возникновения нарушения. Этот план должен включать чёткие протоколы обнаружения кибер-инцидентов, реагирования на них и восстановления после них.
- **Удалённый мониторинг и управление**: Учитывая изоляцию и суровые условия Антарктиды, надёжные инструменты удалённого мониторинга и управления необходимы для поддержания мер кибербезопасности и эффективного реагирования на инциденты.

F. Международное сотрудничество

- **Глобальные стандарты и протоколы**: Международное сотрудничество имеет жизненно важное значение для установления единых стандартов и протоколов кибербезопасности, выходящих за рамки национальных границ. Сотрудничество между государственными учреждениями, заинтересованными сторонами отрасли и международными партнёрами помогает повышать стандарты кибербезопасности и обмениваться передовым опытом.
- **Отчётность о кибер-инцидентах**: Внедрение обязательной отчётности о кибер-инцидентах, как подчёркивается в недавних указах президента, помогает своевременно выявлять кибер-угрозы и реагировать на них. Это имеет решающее значение для поддержания безопасности морских операций в отдалённых регионах, таких как Антарктида.

VI. Тренинг в особых условиях

Морские компании в Антарктике борются с угрозами кибербезопасности, внедряя комплексные и непрерывные программы обучения для своих сотрудников. Эти программы соответствуют международным стандартам, используют передовые средства обучения и направлены на сокращение человеческих ошибок.

A. Комплексные Учебные программы по кибербезопасности

- **Курсы повышения осведомлённости о кибербезопасности**: Компании предоставляют

онлайн-курсы, специально разработанные для членов экипажей судов. Эти курсы охватывают обширные знания о морской кибербезопасности, включая типы информации, уязвимой для кибер-атак, этапы кибер-атаки и меры по смягчению последствий.

- **Целостные подходы к обучению**: Учебные программы разработаны, чтобы охватывать широкий круг тем, включая новейшие риски безопасности, политики и процедуры. Это помогает уменьшить количество человеческих ошибок, которые являются одной из основных причин инцидентов в области кибербезопасности на судах.

B. Регулярные и обновленные Учебные занятия

- **Непрерывное образование**: регулярное обновление учебных программ с учётом новейших угроз кибербезопасности и передовых практик гарантирует, что сотрудники остаются бдительными и информированными. Это включает в себя обучение новейшим тактикам фишинга и другим распространённым кибер-угрозам.

- **Обучение реагированию на инциденты**: сотрудники обучаются тому, как надлежащим образом реагировать на инциденты в области кибербезопасности, что помогает минимизировать ущерб и обеспечить бесперебойное выполнение критически важных операций.

C. Соответствие международным стандартам

- **Руководящие принципы ИМО**: учебные программы приведены в соответствие с руководящими принципами Международной морской организации (ИМО) по управлению кибер-рисками на море. Настоящие руководящие принципы содержат рекомендации высокого уровня и функциональные элементы для минимизации рисков и воздействия на операции, связанные с судоходством, безопасность.

- **Конвенция ПДНВ**: международная конвенция о стандартах подготовки, сертификации и несения вахты для моряков (STCW) пересматривается с целью включения "осведомлённости о кибербезопасности" в качестве отдельной области развития компетенций. Это гарантирует, что моряки будут обучены цифровым навыкам, коммуникациям, управлению информацией и способности адаптироваться к меняющимся условиям работы.

D. Использование передовых средств обучения

- **«Тренажёры»**: использование «тренажёров» в учебных программах помогает сотрудникам понимать реальные кибер-угрозы и управлять ими. Такой подход имеет решающее значение для развития практических навыков выявления кибер-угроз и смягчения их последствий.

- **Искусственный интеллект и машинное обучение**: передовые системы обнаружения угроз, использующие ИИ и ML, интегрируются в учебные программы. Эти системы помогают сотрудникам научиться обнаруживать необычное поведение, которое может указывать на кибер-угрозу.

E. Сокращение человеческих ошибок

- **Информационные кампании**: регулярные информационные кампании и учебные занятия помогают снизить количество человеческих ошибок за счёт повышения осведомлённости о рисках, политиках и процедурах безопасности.

- **Симуляции фишинга**: проведение симуляции фишинга в рамках обучения помогает сотрудникам распознавать попытки фишинга и предотвращать их.

VII. Изменения в морской отрасли Антарктиды

Новейшие правила кибербезопасности для морской отрасли в Антарктике разработаны на основе сочетания международных: Система Договора об Антарктике (ATS) и Конвенция Организации Объединённых Наций по морскому праву (UNCLOS), а также конкретных руководящих принципов Международной морской организации (IMO). Кроме того, недавние указы Президента США ввели новые требования и стандарты кибербезопасности, подчёркивая необходимость комплексного управления кибер-рисками и отчётности об инцидентах. Международное сотрудничество по-прежнему имеет важное значение для установления и поддержания эффективных мер кибербезопасности в морской отрасли.

A. Система Договора об Антарктике (CAP)

- **Обзор**: CAP представляет собой международную систему соглашений, регулирующих деятельность в Антарктике. Он включает положения о мирном использовании континента, защите окружающей среды и содействии научным исследованиям.

- **Безопасность на море**: CAP требует, чтобы все суда, заходящие в территориальные воды Антарктики и покидающие их, были зарегистрированы в Секретариате Договора об Антарктике. Он также предусматривает обеспечение соблюдения правил безопасности и мониторинг судов для обеспечения соблюдения правил международного судоходства.

B. Конвенция Организации Объединенных Наций по морскому праву (UNCLOS)

- **Морское право**: UNCLOS содержит всеобъемлющий свод норм, регулирующих море и его ресурсы, включая право стран на морское судоходство и ответственность за защиту и сохранение морской среды.

- **Положения о кибербезопасности**: хотя UNCLOS в первую очередь затрагивает традиционные вопросы безопасности на море, её принципы являются основополагающими для разработки мер кибербезопасности в морской сфере. В нем подчёркивается необходимость сотрудничества между государствами для обеспечения

безопасности на море, что включает в себя противодействие кибер-угрозам.

C. Руководящие принципы Международной морской организации (ИМО)

- **Управление кибер-рисками**: ИМО представила руководящие принципы по управлению кибер-рисками для судов и судоходства, включая требование к компаниям разрабатывать планы управления кибер-рисками. Настоящие принципы содержат рекомендации высокого уровня и функциональные элементы для минимизации рисков и воздействия на операции, связанные с судоходством.
- **MSC-FAL.1-Circ.3-Rev.2**: настоящее руководство по управлению кибер-рисками на море, выпущенное в июле 2022 года, содержит рекомендации высокого уровня и в значительной степени зависит от интерпретации физического лица или компании, его применяющей.

D. U.S. Указы и федеральные правила

- **Распоряжение администрации Байдена**: 21 февраля 2024 года президент Байден подписал Распоряжение, направленное на повышение кибербезопасности портов США и морских цепочек поставок. Этот приказ вводит новые требования и стандарты безопасности для заинтересованных сторон Морской транспортной системы США (MTS) и повышает полномочия береговой охраны США по противодействию кибер-угрозам.
- **Отчётность о кибер-инцидентах**: исполнительный указ предписывает сообщать о фактических или потенциальных кибер-инцидентах, которые могут поставить под угрозу гавани, портовые или прибрежные сооружения. Это включает в себя обмен отчётами с Агентством по кибербезопасности и инфраструктурной безопасности (CISA) и Федеральным бюро расследований (ФБР).

E. Международное сотрудничество

- **Глобальные стандарты и протоколы**: учитывая глобальный характер морских операций, международное сотрудничество имеет важное значение для установления единых стандартов и протоколов кибербезопасности. Сотрудничество между госучреждениями, заинтересованными сторонами отрасли и международными партнёрами имеет решающее значение для повышения стандартов и обмена передовым опытом.
- **Регулирующие органы**: нормативная база морской кибербезопасности всё ещё развивается, что приводит к несоответствиям и проблемам с внедрением. ИМО и другие международные организации продолжают уточнять и обновлять руководящие принципы для решения растущих кибер-угроз в морской отрасли.

VIII. Экономические последствия

Кибер-атаки на морскую отрасль в Антарктиде могут иметь далеко идущие экономические последствия, включая сбои в научных исследованиях и операциях, увеличение операционных расходов, сбои в цепочке поставок, потерю конфиденциальных данных и интеллектуальной собственности, а также усиление нацбезопасности и геополитической напряжённости.

A. Срыв научных исследований и операций

- **Влияние на исследовательские миссии**: атаки могут нарушить работу исследовательских судов и станций, что приведёт к задержкам или отмене научных миссий к потере ценных исследовательских данных и увеличению затрат, связанных с перепланированием и продлением миссий.
- **Эксплуатационные задержки**: сбои в работе навигационных систем, сетей связи и других критически важных эксплуатационных технологий могут привести к значительным задержкам в морских операциях. Это увеличит эксплуатационные расходы и снизит эффективность исследовательских миссий и миссий по снабжению.

B. Увеличение Эксплуатационных расходов

- **Затраты на смягчение последствий и восстановление после кибер-атак**: затраты, связанные со смягчением последствий кибер-атак и восстановлением после них, могут быть значительными. Сюда входят расходы, связанные с реагированием на инциденты, восстановлением системы и внедрением дополнительных мер безопасности для предотвращения будущих атак.
- **Страховые взносы**: кибер-атаки могут привести к повышению страховых взносов для морских компаний, работающих в Антарктиде. Страховщики могут увеличить страховые взносы для покрытия повышенного риска кибер-инцидентов, увеличивая общие операционные расходы.

C. Сбои в цепочке поставок

- **Влияние на логистику**: атаки нарушают цепочку поставок, и имеют влияние на транспортировку товаров и предметов первой необходимости в Антарктиду и обратно. Это приводит к нехватке важнейших поставок, увеличению транспортных расходов и задержкам в доставке товаров.
- **Волновые эффекты для экономики**: сбои в цепочке поставок могут оказывать волновой эффект на экономику в целом, затрагивая отрасли, которые зависят от своевременных поставок товаров и материалов. Это приведёт к увеличению затрат и снижению производительности во многих секторах.

D. Потеря конфиденциальных данных и интеллектуальной собственности

- **Утечка данных**: кибер-атаки приводят к краже конфиденциальных данных, включая результаты

исследований, конфиденциальную информацию и личные данные членов экипажа и исследователей. Потеря таких данных может иметь значительные экономические последствия, включая потерю конкурентного преимущества и потенциальную юридическую ответственность.

- **Кража интеллектуальной собственности**: кража интеллектуальной собственности: запатентованные исследовательские данные и технологические инновации, подорвёт экономическую ценность научных исследований и разработок в Антарктике.

E. Влияние на нацбезопасность и геополитические интересы

- **Геополитическая напряжённость**: кибер-атаки на морские операции в Антарктиде могут усугубить геополитическую напряжённость, особенно если они приписываются субъектам национального государства. Это приведёт к увеличению расходов на оборону и безопасность, поскольку страны стремятся защитить свои интересы в регионе.
- **Стратегические уязвимости**: срыв морских операций может выявить стратегические уязвимости, потенциально влияющие на национальную безопасность и экономическую стабильность. Это может привести к увеличению инвестиций в кибербезопасность и оборонные меры, отвлекая ресурсы от других важных областей.

IX. Неэкономические последствия

Неэкономические последствия кибер-атак на морскую отрасль в Антарктиде значительны и многогранны. Они включают угрозы безопасности и жизни людей, ущерб окружающей среде, геополитическую напряжённость, срыв научных исследований и операционные проблемы.

A. Безопасность и человеческая жизнь

- **Безопасность экипажа**: кибер-атаки ставят под угрозу безопасность членов экипажа, нарушая работу критически важных систем, таких как навигация, связь и управление двигателем. Это может привести к авариям, посадкам на землю или столкновениям, подвергая риску жизни.
- **Поисково-спасательные операции**: сбои в работе систем связи и навигации могут затруднить поисково-спасательные операции, затрудняя обнаружение судов, терпящих бедствие, и оказание им помощи. Это приводит к задержке реагирования и увеличению риска для жизни человека.

B. Воздействие на окружающую среду

- **Загрязнение и разливы**: атаки, нарушающие работу систем навигации или управления двигателем, приводят к авариям - разливам нефти или выбросу опасных материалов в хрупкую окружающую среду Антарктики. Такие инциденты имеют долгосрочные пагубные последствия для морских экосистем и дикой природы.
- **Ущерб экосистеме**: регион Антарктики является домом для уникальных и чувствительных экосистем. Аварии, вызванные кибер-атаками, могут нанести значительный ущерб этим экосистемам, оказывая влияние на биоразнообразие и общее состояние окружающей среды.

C. Геополитические последствия и последствия для безопасности

- **Геополитическая напряжённость**: кибер-атаки на морские операции в Антарктиде усугубляют геополитическую напряжённость, особенно если они приписываются субъектам национального государства. Это может привести к увеличению военного присутствия и усилению мер безопасности в регионе, что приведёт к эскалации конфликтов.
- **Национальная безопасность**: срыв морских операций может выявить стратегические уязвимости, влияющие на национальную безопасность. Это особенно актуально для стран, имеющих значительные интересы в Антарктике, поскольку кибер-атаки могут подорвать их способность защищать и отстаивать свои претензии и интересы в регионе.

D. Срыв научных исследований

- **Влияние на исследовательские миссии**: кибер-атаки нарушают работу исследовательских судов и станций, что приведёт к задержкам или отмене научных миссий, к потере ценных исследовательских данных и мешает научному прогрессу в понимании изменения климата, морской биологии и других важнейших областей.
- **Целостность данных**: кибер-атаки ставят под угрозу целостность научных данных, что приводит к неточным или неполным результатам исследований. Это может подорвать доверие к научным исследованиям и повлиять на политические решения, основанные на таких данных.

E. Операционные и логистические проблемы

- **Сбои в работе**: кибер-атаки могут нарушить повседневную работу морских судов, затрагивая все – от навигации до обработки грузов. Это может привести к значительным логистическим проблемам, включая задержки в доставке основных материалов и оборудования на исследовательские станции.
- **Нарушение связи**: сбои в системах связи приводят к изоляции судов и исследовательских станций, затрудняя координацию действий и реагирование на чрезвычайные ситуации. Это увеличивает риск несчастных случаев и затрудняет эффективное управление в кризисных ситуациях.

Больше материалов: Boosty | Sponsr | TG

ИРОНИЯ БЕЗОПАСНОСТИ