**УДК 004.023**
DOI: 10.34046/aumsuomt104/26

# ПРОТИВОСТОЯНИЕ КИБЕРПИРАТСТВУ НА МОРСКИХ ПУТЯХ

*А.В. Лошкарев, аспирант*
*Н.Д. Акмайкин, аспирант*

В статье приведены научно обоснованные действия по кибербезопасности. Все пункты сконструированы грамотно и последовательно. Одним из действий по предотвращению кибервзломов является создание пароля, который характеризуется своей надежностью. Выведена формула информационной энтропии – меры сложности пароля. В статье приведено два графика «Диаграмма зависимости энтропии от сложности созданного пароля» и «Диаграмма зависимости надежности созданного пароля от энтропии». Графики позволяют выявить зависимость надежности пароля от его сложности. С каждым годом учащаются случаи кибепреступлений на море. В статье приведены рекомендации для моряков, судов и судоходных компаний по кибербезопасности. Киберпираты, осваивая направление «хакерство», все ближе подбираются к нужным им информационным ресурсам и в связи с этим в статье говорится о действиях при кибервзломах и плане защиты личной, судовой или компанейской системы от непредвиденных кибератак. Каждая судоходная компания вместе с членами экипажа судов должны рассматривать функции управления рисками, что позволит повысить надежность системы. В связи с вышеизложенным можно сделать вывод: выполняя все меры предосторожности, рекомендации по предотвращению кибепреступлений и рассматривая функции управления рисками можно избежать кибератаки и потерю важных информационных данных, что приводит зачастую к потере денежных ресурсов.

**Ключевые слова**: Киберпреступление, кибербезопасность, вирус, антивирусная программа, кибератака, кибервзлом, план по кибербезопасности, конфиденциальные информационные данные

# CONFRONTATION CYBER PIRACY ON SEAWAYS

*A.V. Loshkarev, N. D. Akmaykin*

The article presents effective scientifically based security activities. All items are designed correctly and consistently. One of the actions to prevent cyber hacking is creating of a password, which is characterized by its reliability. The formula of information entropy has been created – measures of complexity of password. The article provides two graphs 'The diagram of the dependence of entropy from the complexity of the created password' and "diagram of the reliability of the created password from entropy". Graphs allow identifying the dependence of the password reliability from its complexity. Every year cases of cybercrimes at the sea are rapidly. The article provides recommendations for sailors, ships and shipping companies on cybersecurity. Cyber Pirates, developing the direction of "hacking", closely selected to the information resources needed for them, and thereby the article talks about actions at cyber hacking and protection plan of personal, shipping and companying system from unexpected cyber attack. Each shipping company together with crew members of ships should consider risk management functions, which will improve the reliability of the system. In relation to above we can conclude: if perform all precautions, recommendations for preventing cybercrime and consider risk management functions, we can avoid cyber attacks and loss of important information data, which often leads to the loss of money resource.

**Key words:** Cyber crime, cyber security, virus, antivirus program, cyber attack, cyber hacking, cyber security plan, confidential informational data.

## Введение

Море – это одна из значимых частей нашей жизни, благодаря которой осуществляется перевозка различного груза, документации или круиз по миру. Именно поэтому с каждым годом большинство судов оснащаются улучшенной электронной системой и оборудованием, упрощающим работу моряку. По нынешней статистике 63% навигационной инфраструктуры упростилось для судоводителя и облегчило ему задачу, ведь, например, в настоящее время моряку не приходится брать в руки секстант и вычислять местоположение судно, за него это делает GPS система. Также можно сказать, что с появлением ECDIS, бумажные карты вышли из эксплуатации, что упрощает задачу при корректуре карт.

Но, несмотря на все преобразования, обновления и улучшения электронных приборов, киберпиратство стремительно врывается в инфраструктуру перевозок, что приводит к значительным информационным и материальным потерям, как для моряков, так и для судоходства.

С каждым годом киберпираты становятся изощренней, умнее и хитрее. Они создают различные вирусы и вредоносные программы, которые способны обходить антивирусные системы, врываться в ядра компьютерной информационной технологии. Злоумышленники всегда действуют по разным схемам и преследуют разные мотивы. Каждый кибепреступник может как выкрасть важную информацию, например, для дальнейшего шантажа моряка, судоходной компании, или целью может служить уничтожение судовой системы, так и фальсифицировать данные для приведения преступного плана в действие.

**1. Действия по кибербезопасности против киберпреступлений**

Каждый моряк может обеспечить безопасность его системы против киберпреступлений, направленных на получение собственной выгоды.

В первую очередь рекомендуется создать надежный пароль для доступа к системе и хранить его в конфиденциальности. Но по статистике 60% людей для простоты и удобства хранят свои пароли на телефонах, вебсайтах и в других ненадежных местах, что повышает риск взлома системы путем воровства паролей, ведущих к личной и важной информационной структуре.

Для надежности необходимо создавать сложные и разнообразные для всех имеющихся используемых веб-сайтов пароли. Каждая киберструктура рекомендует использовать заглавные и маленькие буквы, знаки и цифры – это усилит защиту конфиденциальных данных.

Надежность созданного пароля можно рассчитать через его сложность.

Любой пароль независимо от его применения можно оценить в информационной энтропии – мера непредсказуемости, измеряемая в битах.

Вместо количества попыток, предпринимаемых для взлома пароля, вычисляется логарифм по основанию 2 от этого числа – полученное значение называется количеством «битов энтропии» в пароле.

$$E = \log_2 M^N = N \log_2 M \qquad (1)$$

где E – информационная энтропия, измеряемая в битах, M – количество возможных символов, N – количество символов, используемых в пароле.

Например, при использовании в пароле арабских цифр энтропия на 1 символ будет составлять 3,322 бита, при использовании английского алфавита энтропия будет иметь значение 4,000 бит на 1 букву.

Следовательно, при использовании в пароле различных групп символов формула представит следующий вид:

$$E = \log_2 M_1^{N_1} + \log_2 M_2^{N_2} + \cdots + \log_2 M_n^{N_n} + = N_1 \log_2 M_1 + N_3 \log_2 M_3 + \cdots + N_n \log_2 M_n \qquad (2)$$

Из формулы (1) видно, чем количество возможных символов выше, тем больше значение информационной энтропии.

Из формулы (2) видно, чем больше количество используемых символов в пароле, тем выше значение информационной энтропии.

С рисунка 1 и 2 видно, что надежность созданного пароля зависит от его сложности.

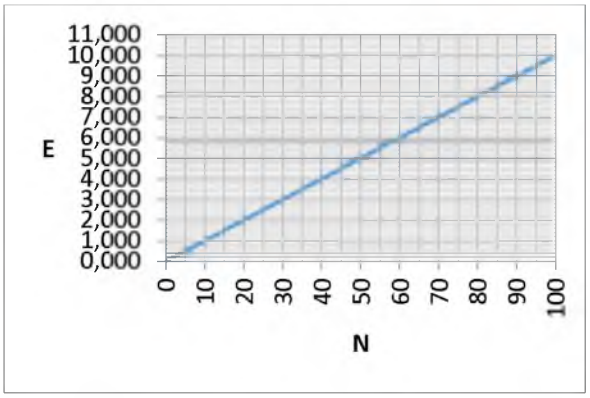


Рисунок 1 – Диаграмма зависимости энтропии от сложности созданного пароля


Рисунок 2 – Диаграмма зависимости надежности созданного пароля от энтропии

Еще одним этапом для предотвращения киберпреступлений является недопустимость открытия подозрительных сайтов и сообщений, особенно на судовом сервере. Некоторые киберпреступники практикуют метод получения конфиденциальной информации путем отправки на судовые серверы и почтовый ящик, различные сообщения, открыв которые автоматически запускается вирус-разведчик, въедающийся в ядро компьютерной системы [1, 3, 6].

Необходимо избегать открытия смс или прием телефонных звонков от неизвестных и странных номеров телефонов.

Причиной этого является то, что зачастую хакеры используют смс или звонки на номера телефонов, которые ведут к попаданию вредоносных ПО и вирусов в устройство. Особенно это происходит, когда моряки покупают карты в разных портах мира. Одно нажатие через смс или прием странного звонка может загрузить на телефон вредоносное ПО-разведчик.

Также еще одним способом предотвращения кибератаки является отсутствие в использовании непроверенных дисков или жестких переносных носителей. Не рекомендуется вставлять в USB порт какие-либо информационные носители посторонних лиц, даже при установленной и обновленной антивирусной программой [1, 2, 4].

Используя бесплатный, в легком доступе и незапароленный Wi-Fi необходимо быть осторожным, ведь это основное поле для хакеров.

Любая судоходная компания должна обеспечить безопасность судна от кибератак.

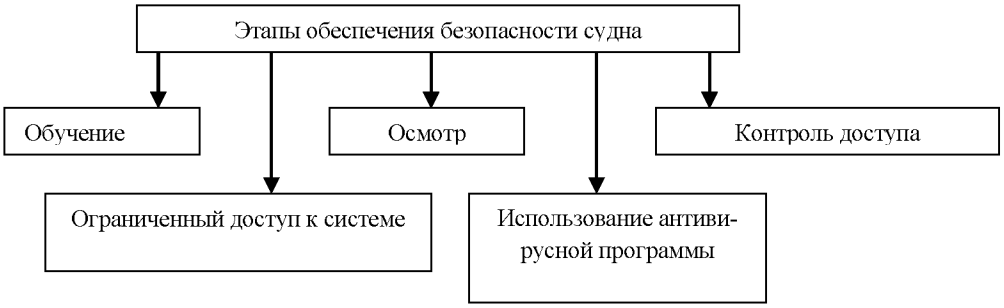


Рисунок 3 - Этапы обеспечения безопасности судна

1. Обучение членов экипажа от предотвращения кибератак

Человеческий фактор – одна из значимых факторов в проблемах кибербезопасности на борту судов. 95% воровства ценной информации и кибервзломов системы происходит из-за невнимательности моряков или пренебрежения киберруководством [3, 5].

Программа обучения, обеспечивающая компанией, должна покрывать 3 основных района:

1) Этапы предотвращения атак

2) Пути обнаружения вредоносного ПО или вирусы внутри системы, или возможные подозрительные ПО или файлы

3) Способы излечения атакуемой системы и восстановление необходимых условий (данных)

В связи с этим всем обучение должно быть проведено экипажу на разных уровнях и должно включать предупредительные меры предотвращения, также как антивирус и антивирусные ПО, дублирование основных файлов,…

2. Регламентированный и сложный контроль доступа

Компания должна установить на судне систему, которая регламентирована и требует разрешения на разных уровнях.

Капитан и все высококвалифицированные специалисты на судне должны быть обучены относительно иерархии онлайн системы, которую необходимо придерживаться.

3. Осмотр

Судоходная компания должна регулярно проводить осмотр системы информационной технологии, установленной на борту, текущий статус антивирусной программы и состояние самой системы, т.е. является ли система зараженной, т.к. без этих действий экипаж судна может никогда и не узнать в случае заражении судовой системы.

4) Ограниченный доступ к системе

Моряки, находясь на борту судна, могут входить в судовой компьютер для рабочего и персонального использования. Компании рекомендуется держать простое обеспечение подключенную судовую систему на разных сетях, системах или компьютерах, использующихся для обучения и персонального использования. Судовая команда должна гарантировать, что не одно персональное средство, жесткий диск, usb, cd и многое другое устройство, способное занести вирус в систему, не будут вставлены в судовую сеть без особого разрешения.

Также возможен тот факт, что посетители (портовые власти, агент…) будут требовать / просить доступ к компьютеру или принтеру с целью занесения своей информации через переносной носитель. В таких случаях, компьютер, не подключенный к судовой контролируемой сети, может быть использован.

Во избежание незаконного доступа, переносные блокаторы средств массовой информации должны быть использованы на всех других доступных компьютерах или портовых сетей.

5) Использование последней антивирусной программы

Антивирусная программа – компьютерная программа, предназначенная для обнаружения, реагирования и удаления любых злостных ПО с вирусами или вредоносными ПО [2, 4].

Антивирусная программа реагирует на зараженные объекты и блокирует доступ к ним.

Компания должна гарантировать, что подключенные системы обеспечены брандмауэр (межсетевой экран – аппаратные или программные средства межсетевой защиты) и обновлен.

**2. Действия при кибератаках или ответ кибератакам**

Существует ряд рекомендуемых действий, направленных против кибепресуплений.

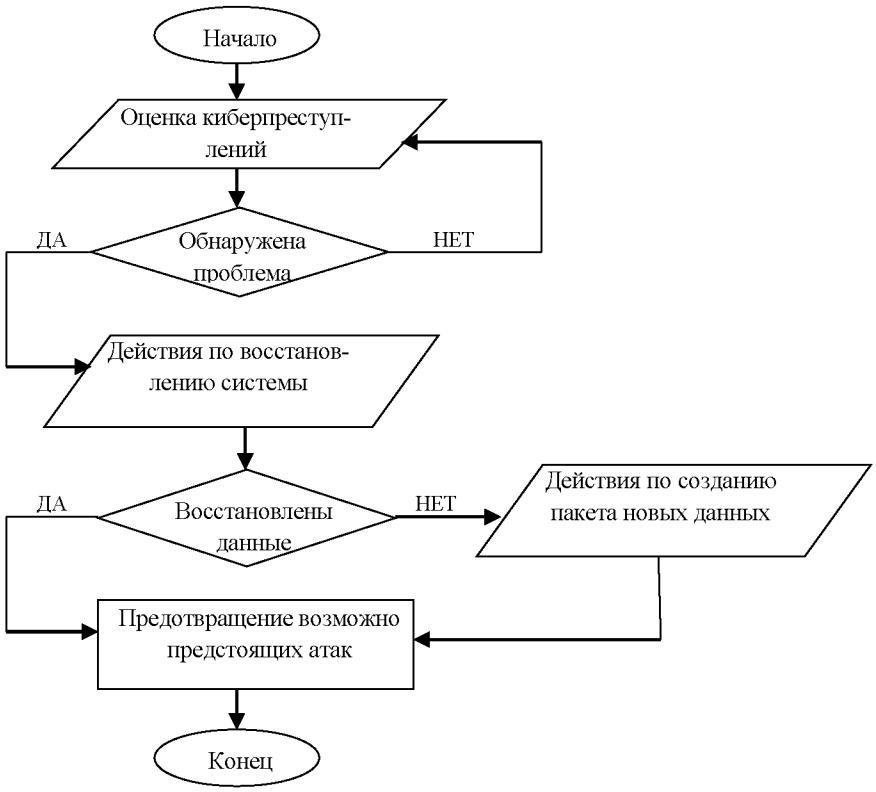


Рисунок 4 – Схема «Ответ кибератакам»

1) Обнаружить проблему через оценку

Любая специализированная команда IT экспертов для обнаружения проблем решают алгоритмы по обнаружению кибернедочетов путем оценки киберпреступлений [2, 3]. Для лучшего понимания и представления о кибервзломах, рекомендуется ответить на следующие вопросы для полного понимания изъянов системы:

- Какие были причины для инцидента?
- Какой тип атаки и уровень угрозы?
- Какой объем данных заражен?

2) Возобновить важные данные

Если возможно отдел IT должен действовать быстро, чтобы вернуть IT и OT данные разделением чувствительных данных от сети, удалением зараженных файлов, установление заплаты (или патч – программное обеспечение для устранения ошибок защиты). Приоритет этой платформы – восстановить систему в рабочее состояние в кратчайший срок.

3) Предотвращение повтора атак

Для судов, восстановление от атаки недостаточно. Важнейшим шагом к предотвращению атак в будущем является расследование киберпреступлений, необходимое для понимания причин возникновения данного инцидента и последовательности действий, ведущих к кибербезопасности.

Люди, работающие на судах, должны быть осведомлены о результатах расследования и знать уязвимости, которые могут привести к таким атакам в будущем.

Компания должна обеспечить возобновление данных и разработать план предотвращения, чтобы уменьшить и минимизировать эффект от таких атак в будущем.

**3. План защиты от непредвиденных кибератак**

План по предотвращению атак от судоходной компании – одна из важных мер по защите судна от кибернаподения.


Рисунок 5 – Функции управления рисками

Согласно руководства ИМО, 5 функциональных подходов к управлению киберрисками должны быть выбраны, следуя инструкциям, упомянутых во всех частях этого руководства [2, 4, 6].

5 функций управления рисками:

1. Распознание систем, политик, процедур,

которые уязвимы к атакам

2. Предотвращение – приведенные защитные меры, такие как обучение, техническая защита, контроль и т.д.

3. Обнаружение – системы и процессы, чтобы обнаружить киберслучаи, как внедрение обнаружительных систем, анализирование отклонения от норм и т.д.

4. Ответ – план по организации отвечать кибератакам. Например, связь, планирование ответа и т.д.

5. Восстановление – процедуры по восстановлению данных и возврат системы и т.д.

Но также рекомендуется к рассмотрению шестой пункт, в который можно отнести план по улучшению защитных мер от кибератак.

План по кибербезопасности должен содержать:

1. Описание различных основных систем безопасности и оборудования

2. Политику и процедуры

3. Роль и ответственность каждого члена экипажа

4. Анализ уязвимостей, системы и процедуры для всех плановых работ судна и береговой возможной помощи.

5. Процесс и описание оценки рисков

6. Реестр рисков включает допустимости рисков и оценки рисков

7. Метод деления информации кибербезопасности

Осуществление плана кибербезопасности

План по кибербезопасности и защите должна объединять следующее:

1. План работы и поддержание

2. Реестр контроля и информационная система оборудования

3. Реестр ПО и его усовершенствования

4. Доклад на тестировании уязвимостей

5. Запись киберинциндентов

6. Полная детализация удаленных входов

7. План и политика управления конфигурации ПО

8. Диаграмма сети для IT и OT систем

9. Информация на уязвимое ПО и ценные данные аппаратного обеспечения (АО)

10. Тестирование процедур и записей для каждой смены в ПО и АО двух систем – IT и OT

При осуществлении всех условий содержания и осуществления плана по кибербезопасности система будет защищена от кибервзломов и будет соответствовать всем требованиям необходимых для ее защиты.

**Заключение**

Каждая система, сеть, программа, аппаратура требует полной защиты от различных сбоев, перегрузок и киберпреступлений, направленных на взлом информационных данных с целью выкупа, шантажа и много другого. Именно по этой причине необходимо соблюдение правил и условий по кибербезопасности, направленных на борьбу с кибермошенничеством и сохранение конфиденциальных информационных данных в личном пользовании.

Любая информационная защита требует разработку и выполнения действий по предотвращению кибепреступлениий и борьбы с ними. С этой целью создается и постоянно обновляется и модернизируется план по кибербезопасности, в котором включен ряд действий по сохранению личных данных.

В море, как и на суше, важную роль играет подготовка и квалификация как офицерского, так и рядового состава. Рекомендуется всем судоходным компаниям, как минимум, раз в год проводить курсы по кибербезопасности для всех моряков, где уделять особое внимание всем усовершенствованиям и новшествам в мире кибертехнологии.

**Литература**

1. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; под ред. акад. Б.П. Смагоринского.– М.: Право и закон, 2014.– 182 с.
2. Авчаров И.В. Борьба с киберпреступностью / И.В. Авчаров. // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф.– М., 2012.– С. 191-194.
3. Raunek Kantharia. A Pocket Guide to Cybersecurity for Seafarers / Raunek Kantharia // Marine Insight, 2018. – 38 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш.– М.: Риор, 2018.– 400 с.
5. Малюк, А.А. Защита информации в информационном обществе: учебное пособие для вузов / А.А. Малюк.– М.: ГЛТ, 2015.– 230 с.
6. Мельников, В.П. Информационная безопасность и защита информации / В.П. Мельников.– М.: Академия (Academia), 2012.– 276 с.

**References**

1. Vekhov V. B. Komp'yuternye prestupleniya: sposoby soversheniya i raskrytiya [Computer crimes: ways of committing and disclosing] / V.B. Vekhov; Pod red. akad. B.P. Smagorinskogo. - M.: Pravo i zakon, 2014.- 182 s.
2. Avcharov I.V. Bor'ba s kiberprestupnost'yu [Fight against cybercrime] / I.V. Avcharov. // Informatizaciya i informacionnaya bezopasnost' pravoohranitel'nyh organov [Informatization and information security of law enforcement agencies]. XI mezhd. konf. - M., 2012. - S. 191-194.
3. Raunek Kantharia. A Pocket Guide to Cybersecurity for Seafarers / Raunek Kantharia // Marine Insight, 2018. – 38 s.
4. Baranova, E.K. Informacionnaya bezopasnost' i zashchita informacii: Uchebnoe posobie [Information Security and Information Protection: A Study Guide] / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 s.
5. Malyuk, A.A. Zashchita informacii v informacionnom obshchestve: Uchebnoe posobie dlya vuzov [Information Security in the Information Society: A Textbook for Universities] / A.A. Malyuk. - M.: GLT, 2015. - 230 s.
6. Mel'nikov, V.P. Informacionnaya bezopasnost' i zashchita informacii [Information security and information protection] / V.P. Mel'nikov. - M.: Akademiya (Academia), 2012. - 276 s.