Лекция 3. (продолжение). Устойчивость судовых систем и инфраструктуры. Судовые активы и кибербезопасность.

Субъекты угроз можно разделить на одну из категорий, которые подробно описаны далее:

- (а) отдельные лица, например, «сценаристы» и инсайдеры;
- (б) группы активистов, также известные как «хактивисты»;
- (в) коммерческие конкуренты;
- (г) киберпреступники;
- (д) террористы;
- (е) национальные государства и субъекты, спонсируемые государством.

- **Группы активистов**

Эти группы, которых часто называют хактивистами,

состоят из идеологически мотивированных людей, которые могут образовывать динамические группы или подгруппы. Их действия эффективны в сети протестов, которые могут иметь цель нарушить работу систем или получить конфиденциальную информацию для публикации или распространения, чтобы изменить по своему усмотрению их цель (цели).

- **Участники**

Эта группа обычно представляет собой крупные корпорации, стремящиеся создать конкурентное преимущество.

- **Киберпреступники**

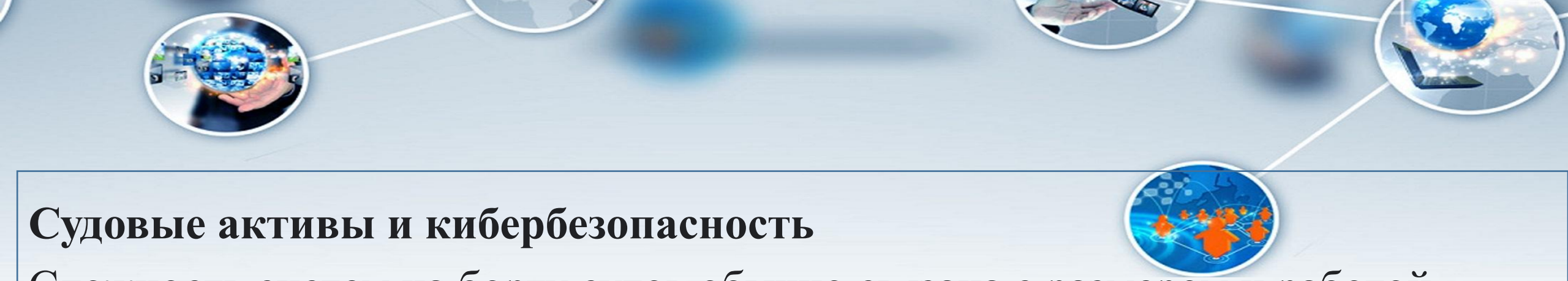
Это изощренные преступные группы, осуществляющие широкий спектр незаконных ИТ-операций. Мотивация состоит в том, чтобы получить прибыль от незаконной деятельности, и их основное внимание уделяется мошенничеству, кражам со счетов и краже интеллектуальной собственности.

- **Террористы**

Террористы все больше узнают об ИТ и уже широко используют Интернет для распространения пропаганды и в коммуникационных целях. Хорошо финансируемые группы могут воспользоваться услугами, предлагаемыми киберпреступниками, искать поддержки от национального государства или поощряя внутренних членов использовать эти методы нападения.

- **Национальные государства и спонсируемые государством субъекты угроз**

Признано, что некоторые национальные государства активно участвуют в кибератаках на широкий круг организаций для получения государственной тайны или конфиденциальной коммерческой информации и интеллектуальной собственности. Они также могут поставить под угрозу доступность критически важной инфраструктуры в других национальных государствах.



Судовые активы и кибербезопасность

Сложность систем на борту судов обычно связана с размером и работой, выполняемой судном в соответствии с контрактом. Однако судну требуются современные информационные системы для обеспечения и управления движением, рулевым управлением, балластом и т. д., как только вы добавляете пассажиров, вы увеличиваете количество и сложность систем для обеспечения объектов и управления человеческим грузом.

В целях разработки соответствующих и соразмерных мер кибербезопасности, каждая из имеющихся технических систем может рассматриваться как находящаяся в основном или непосредственно относится к одной из следующих категорий:

(a) связь - системы, предусмотренные для внутренней связи, связи судно-берег и судно-судно.

(b) навигационные системы - системы, которые либо предназначены непосредственно для навигации, либо предназначены для поддержки судоходства.

(c) заводские системы - системы, используемые для мониторинга и управления любым оборудованием и установками, связанными с общей эксплуатацией судна, не охваченными другими категориями.

(d) системы безопасности - системы, используемые для поддержания целостности, безопасности и / или защищенности корабля и его груза.

(e) грузовые системы - системы, используемые для непосредственного контроля и управления грузом.

(f) системы управления пассажирами - системы, используемые для предоставления услуг / услуг для пассажиров и для поддержания здоровья и благополучия как пассажиров, так и экипажа.

(g) системы доступа пассажира / экипажа - любые системы, предусмотренные для пассажира / экипажа, взаимодействие, не связанное с судовыми операциями или управлением пассажирами / экипажами.

- **Навигационные системы**

Существует ряд навигационных систем и средств навигации,

которые используются, и многие из этих систем подключаются к другим бортовым системам, основными из которых являются связанные различные подсистемы:

(a) Регистратор данных рейса (VDR) - это система регистрации данных, предназначенная для всех судов, требуется для соблюдения требований Международной конвенции ИМО СОЛАС (Резолюция ИМО A.861 (20)) для сбора данных с различных датчиков на борту судна.



Данные, записанные в VDR, могут включать некоторые или все из следующих типов информации:

1. положение, дата, время с помощью GPS;
2. speed log - скорость по воде или скорость по земле;
3. gyro compass - курс;
4. радар;
5. ECDIS - снимок экрана каждые 15 секунд и список навигационных карт в использовании каждые 10 минут или при изменении графика;
6. аудио с мостика, включая крылья мостика;
7. УКВ радиосвязь;
8. эхолот - глубина под килем;
9. main alarms - все обязательные сигналы IMO;
10. проемы корпуса - состояние дверей корпуса, указанное на мостике;

11. состояние водонепроницаемых и противопожарных дверей, указанное на мостике;

12. напряжение корпуса - ускорения и напряжения корпуса;

13. руль направления - приказ и ответная реакция;

14. двигатель / винт - порядок и обратная связь;

15. подруливающие устройства - состояние, направление, количество тяги или оборотов; и

16. анемометр и флюгер - скорость и направление ветра.

Системы судовых установок

На сегодняшний день это самая большая категория, включающая системы, традиционно входящие в машинное отделение, включая двигательную установку, рулевое управление, балласт, выработку и распределение электроэнергии, вентиляцию, смазочное масло, воду (как бытовую, так и питьевую) и др. С включением круиза судов, мы должны признать, что эти плавучие отели могут также иметь эквивалентные системы управления комплексом для управления освещением, отоплением, вентиляцией и кондиционированием и т.д.





Системы безопасности

В эту категорию входят любые системы, которые могут повлиять на безопасность или защищенность судна, груза, пассажиров и экипажа.

Системы включают; ГМССБ (Global Maritime Distress и система безопасности), AMVER (Автоматизированное спасение судов взаимопомощи), SSAS (Система оповещения судна о безопасности), NavTex, радар, сонар, системы оповещения и общей сигнализации, Регистратор данных рейса, TeleMed, Fire и т. д.





Системы управления грузами

В зависимости от типа груза и класса корабля будут использоваться различные системы управления грузом. Танкеры для нефти или сжиженного нефтяного газа, контейнеровозы будут использовать разные системы управления грузами.

Эти системы управления грузами предназначены не только для тех случаев, когда погрузка или разгрузка, но для некоторых грузов также предусмотрена функция постоянного контроля во время транспортировки.

Когда функции судов связаны с перевозкой пассажиров, система управления грузами может также включать эквивалент системы обработки багажа в порту и, конечно, для паромов будут включать системы слежения за транспортными средствами, возможно, подключенными к береговым системам автоматического распознавания номерных знаков (ANPR).

Системы управления пассажирами

- Количество и сложность систем управления

пассажирами будет увеличиваться с количеством и продолжительностью нахождения пассажиров на борту. Используются системы управления пассажирами для предоставления услуг / удобств пассажирам и для поддержания здоровья и благополучия как пассажиров, так и экипажа.

. Системы управления пассажирами - это те системы, к которым не будут иметь доступ напрямую пассажиры и доступ только для экипажа, который несет ответственность за использование систем от имени пассажиров.

Системы доступа пассажиров

- Система доступа пассажира - это любая система, к которой пассажир может получить доступ или интерфейс напрямую с системой. Это включает в себя любую систему, которая позволяет пассажиру взаимодействовать с системой управления пассажирами через портал для онлайн-бронирования или оплаты сервисов.
- В более общем плане эти системы будут включать системы, обеспечивающие доступ к мультимедиа, такие сервисы, как фильмы или музыка, и системы, позволяющие подключаться к Интернету.




Разработка мер защиты и обнаружения

Результатом оценки рисков компании и последующей стратегии кибербезопасности должно стать снижение риска до практически возможного минимума. На техническом уровне это будет включать в себя необходимые действия, которые необходимо выполнить для установления и поддержания согласованного уровня кибербезопасности. Важно определить, как управлять кибербезопасностью на борту, и делегировать обязанности капитану, ответственным сотрудникам и, при необходимости, сотруднику службы безопасности компании.

Вопросы для самоконтроля

1. Дайте определение кибербезопасности.
2. Перечислите атрибуты кибербезопасности.
3. Что вы знаете о мотивации кибератак на судовую систему?
4. Перечислите субъекты киберугроз.
5. Перечислите возможные последствия кибератак на систему.