Лекция 4. 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.

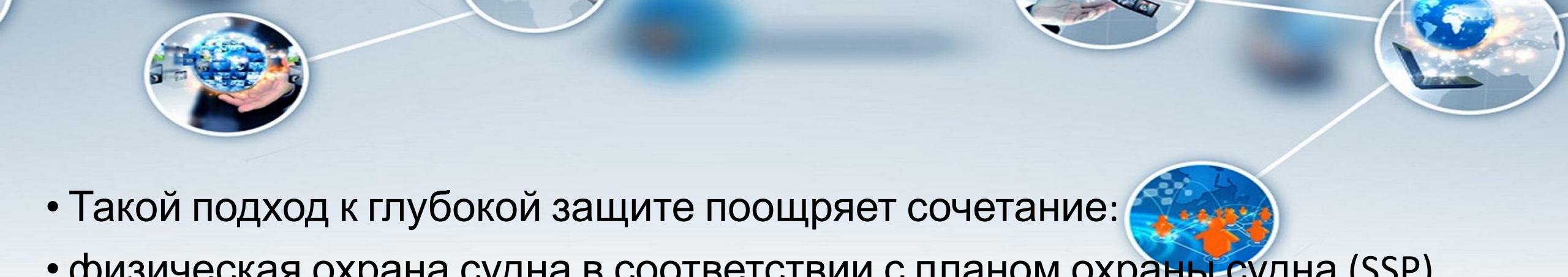
Глубокая и широкая защита

- Важно защитить критически важные системы и данные с помощью нескольких уровней мер защиты, которые учитывают роль персонала, процедур и технологий чтобы:
- ■ увеличить вероятность обнаружения киберинцидента;
- ■ увеличить усилия и ресурсы, необходимые для защиты информации, данных или доступности ИТ- и ОТ-систем.
- Подключенные системы ОТ на борту должны требовать более одной технической и / или процедурной защиты. Защита периметра, такая как брандмауэры, важна для предотвращения нежелательного проникновения в системы, но этого может быть недостаточно для борьбы с внутренними угрозами.

Брандмауэр

Брандмауэр — это защитный экран между глобальным интернетом и локальной компьютерной сетью организации. Он выполняет функцию проверки и фильтрации данных, поступающих из интернета. В зависимости от настроек брандмауэр может пропустить их или заблокировать (например, если обнаружит «червей», вирусы и хакерскую атаку).

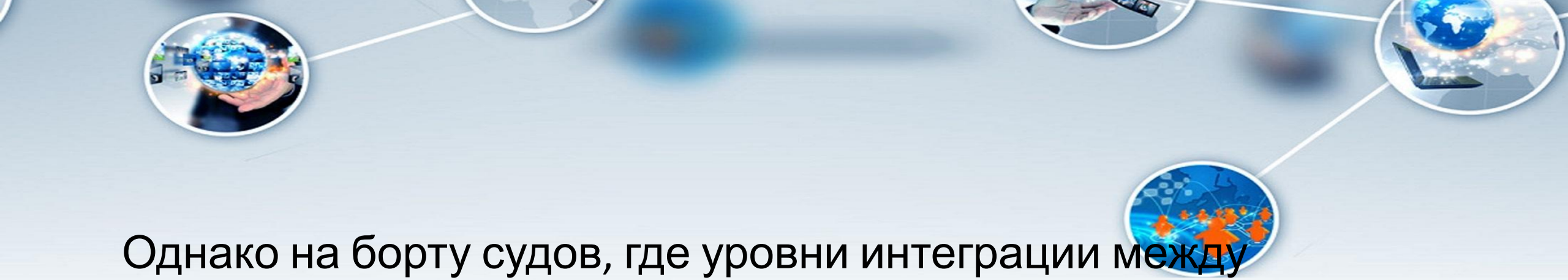
Нужно различать сетевой брандмауэр (или, по-другому, сетевой экран) и брандмауэр, встроенный в операционную систему Windows. В первом случае решение устанавливается на границе (физической или логической) компьютерной инфраструктуры организации и защищает все ПК, подключенные к локальной сети. Это может быть как программное, так и программно-аппаратное решение. Во втором случае это программа, работающая для защиты отдельно взятого компьютера пользователя.



- Такой подход к глубокой защите поощряет сочетание:
- физическая охрана судна в соответствии с планом охраны судна (SSP)
- защита сетей, включая эффективную сегментацию
- обнаружение вторжений
- периодическое сканирование и тестирование уязвимостей
- внесение программного обеспечения в белый список
- доступ и пользовательские элементы управления
- соответствующие процедуры, касающиеся использования съемных носителей и политик паролей
- осведомленность персонала о рисках и знакомство с соответствующими процедурами.

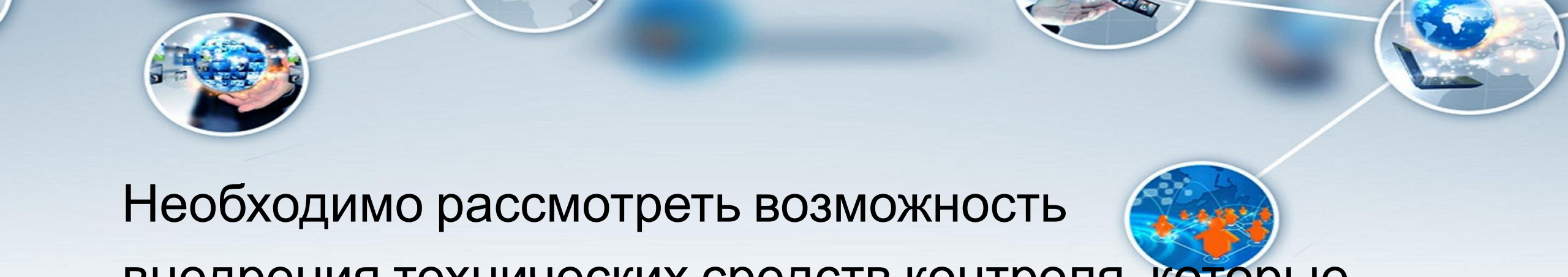

При разработке интеграции между системами следует учитывать модель границ доверия,

в соответствии с которой системы группируются на те, между которыми доверие является неявным (например, пользовательские рабочие станции), и те, между которыми доверие должно быть явным (между компьютерами-мостами и корпоративными сетями). Для больших или сложных сетей моделирование угроз следует рассматривать как деятельность, направленную на понимание того, где должны быть реализованы технические средства управления между системами, чтобы обеспечить защиту в широком смысле.



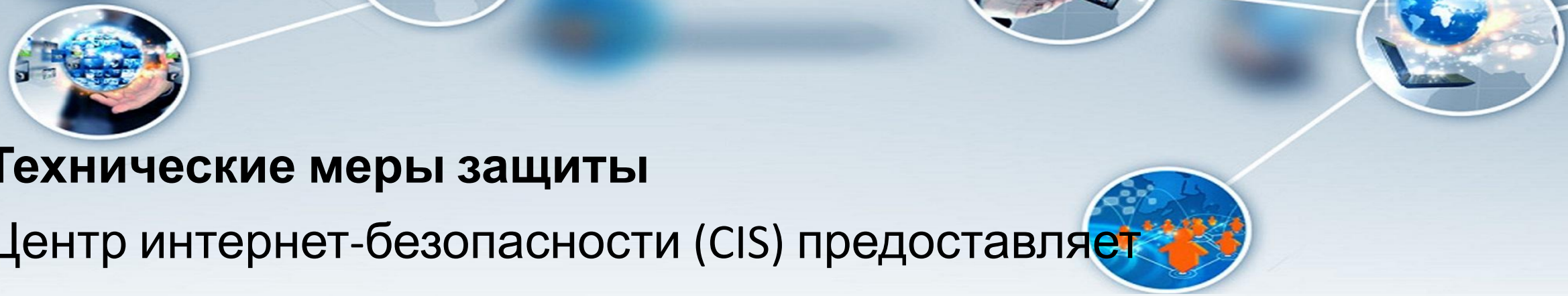
Однако на борту судов, где уровни интеграции между системами могут быть высокими, глубокоэшелонированная защита работает только в том случае, если технические и процедурные меры защиты применяются поэтапно во всех уязвимых и интегрированных системах. Это «защита по всему миру», и она используется для предотвращения любых уязвимостей в одной системе, используемых для обхода мер защиты другой системы.

- Глубокая защита и комплексная защита - это взаимодополняющие подходы, которые при совместной реализации обеспечивают основу для целостного реагирования на управление киберрисками.
- Меры защиты от киберрисков могут быть **техническими** и сосредоточены на обеспечении того, чтобы бортовые системы были спроектированы и настроены таким образом, чтобы быть устойчивыми к кибератакам. Меры защиты также могут быть **процедурными** и должны охватываться политиками компании, процедурами управления безопасностью, процедурами безопасности и средствами контроля доступа.



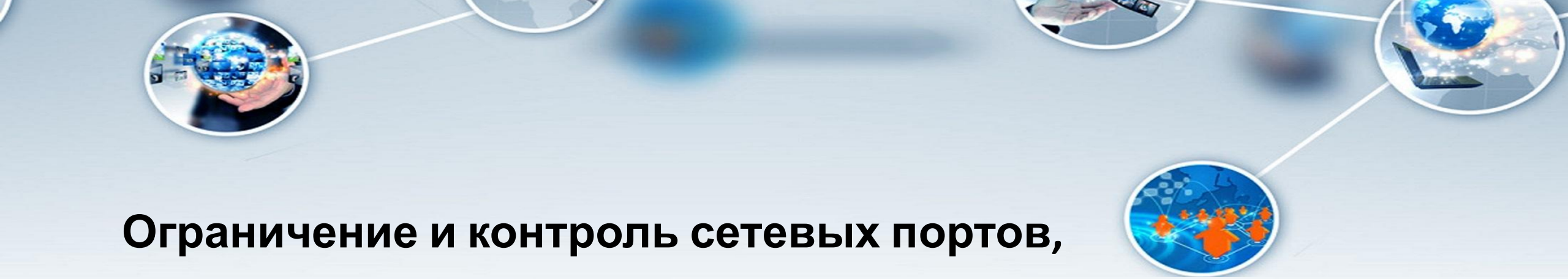
Необходимо рассмотреть возможность внедрения технических средств контроля, которые являются практичными и рентабельными, особенно на существующих судах.

Внедрение мер кибербезопасности должно быть приоритетным, сосредоточив внимание в первую очередь на тех мерах или комбинациях мер, которые приносят наибольшую пользу.



Технические меры защиты

Центр интернет-безопасности (CIS) предоставляет руководство по мерам, которые можно использовать для устранения уязвимостей кибербезопасности. Меры защиты представляют собой список критических средств контроля безопасности (CSC), которые имеют приоритет и проверяются, чтобы гарантировать, что они обеспечивают эффективный подход для компаний для оценки и улучшения своей защиты. CSC включают как технические, так и процедурные аспекты.



Ограничение и контроль сетевых портов, протоколов и сервисов

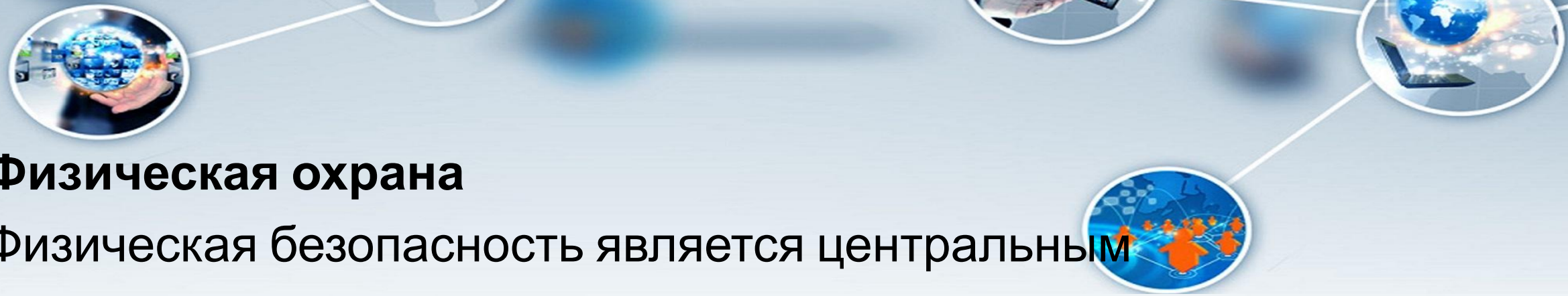
- Списки доступа к сетевым системам могут использоваться для реализации политики безопасности компании. Это помогает гарантировать, что только соответствующий трафик будет разрешен через контролируемую сеть или подсеть в зависимости от политики управления этой сети или подсети.
- Рекомендуется, чтобы маршрутизаторы были защищены от атак, а неиспользуемые порты должны быть закрыты для предотвращения несанкционированного доступа к системам или данным.

Следует определить, какие системы следует подключить к **управляемым или неуправляемым сетям. Управляемые сети** предназначены для предотвращения любых угроз безопасности со стороны подключенных устройств за счет использования межсетевых экранов, шлюзов безопасности, маршрутизаторов и коммутаторов. **Неконтролируемые сети** могут представлять опасность из-за отсутствия контроля за трафиком данных и должны быть изолированы от контролируемых сетей, поскольку прямое подключение к Интернету делает их очень уязвимыми для проникновения вредоносных программ.

- **Эффективное разделение систем на основе необходимых уровней доступа и доверия –**

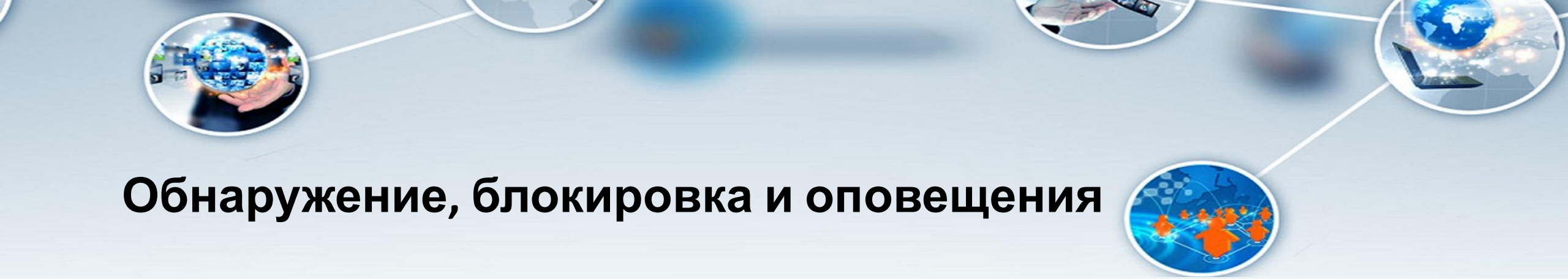
одна из наиболее успешных стратегий предотвращения киберинцидентов. Эффективно разделенные сети могут значительно затруднить доступ злоумышленника к системам корабля и являются одним из наиболее эффективных методов предотвращения распространения вредоносных программ.

Бортовые сети должны быть разделены межсетевыми экранами для создания безопасных зон. Чем меньше каналов связи и устройств в зоне, тем более безопасны системы и данные в этой зоне. **Конфиденциальные и критически важные системы безопасности должны находиться в наиболее защищенной зоне.**



Физическая охрана

Физическая безопасность является центральным аспектом управления киберрисками, и эффективная стратегия защиты основана на обеспечении того, чтобы технические средства контроля невозможно было обойти с помощью тривиальных технических средств. Области, содержащие чувствительные компоненты управления, должны быть надежно заперты, критическое для безопасности оборудование и кабели должны быть защищены от несанкционированного доступа, а физический доступ к чувствительному пользовательскому оборудованию (например, незащищенным портам USB на мостовых системах) должен быть защищен.



Обнаружение, блокировка и оповещения

Выявление вторжений и инфекций - центральная часть процедур контроля. Необходимо установить базовый уровень сетевых операций и ожидаемые потоки данных для пользователей и систем, чтобы можно было установить пороговые значения для оповещения о киберинцидентах. **Ключом к этому будет определение ролей и обязанностей по обнаружению, чтобы обеспечить подотчетность.** Обнаруженные инциденты следует направлять физическому лицу или поставщику услуг, который отвечает за реагирование на этот тип предупреждений.





Спутниковая и радиосвязь

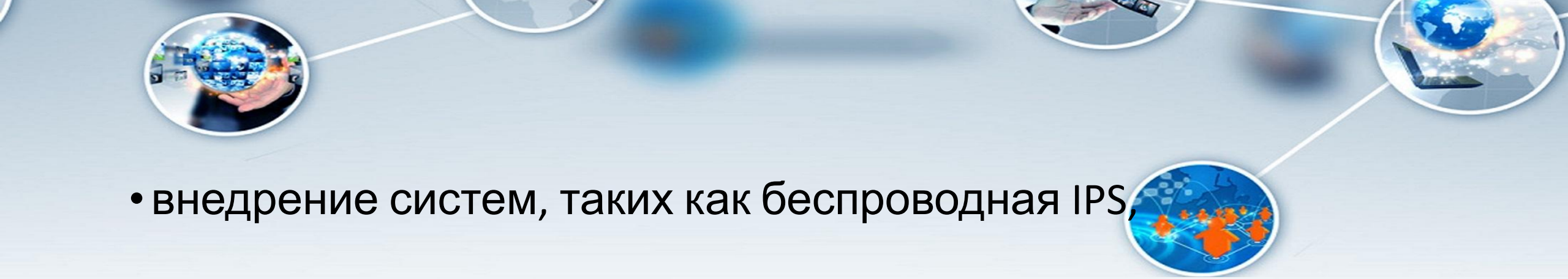
Кибербезопасность радио и спутниковой связи следует рассматривать в сотрудничестве с поставщиком услуг. В связи с этим при установлении требований к защите бортовой сети следует учитывать спецификацию спутниковой линии связи.

При установлении соединения восходящей линии связи для судовых систем навигации и управления с береговыми поставщиками услуг следует учитывать, как предотвратить незаконные соединения, получающие доступ к бортовым системам.

Контроль беспроводного доступа

Беспроводной доступ к сетям на судне должен быть ограничен соответствующими авторизованными устройствами и защищен надежным ключом шифрования, который регулярно меняется. Для управления беспроводным доступом можно учитывать следующее:

- использование корпоративных систем аутентификации, использующих асимметричное шифрование и изолирующих сетей с соответствующими беспроводными выделенными точками доступа (например, ***гостевые сети, изолированные от административных сетей***)



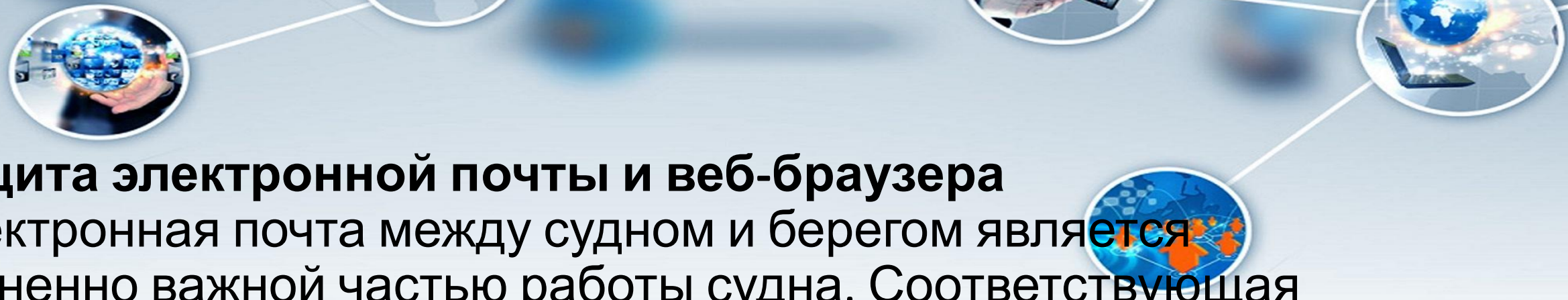
- внедрение систем, таких как беспроводная IPS, которые могут перехватывать неавторизованные точки беспроводного доступа или несанкционированные устройства.
- защита физического взаимодействия между устройствами беспроводного доступа и сетью, такими как сетевые разъемы, сетевые стойки и т. д.), чтобы избежать несанкционированного доступа со стороны

Обнаружение вредоносного ПО

Программное обеспечение для сканирования, которое может автоматически обнаруживать и устранять присутствие вредоносных программ в бортовых системах, ***должно регулярно обновляться.***


Безопасная конфигурация аппаратного и программного обеспечения

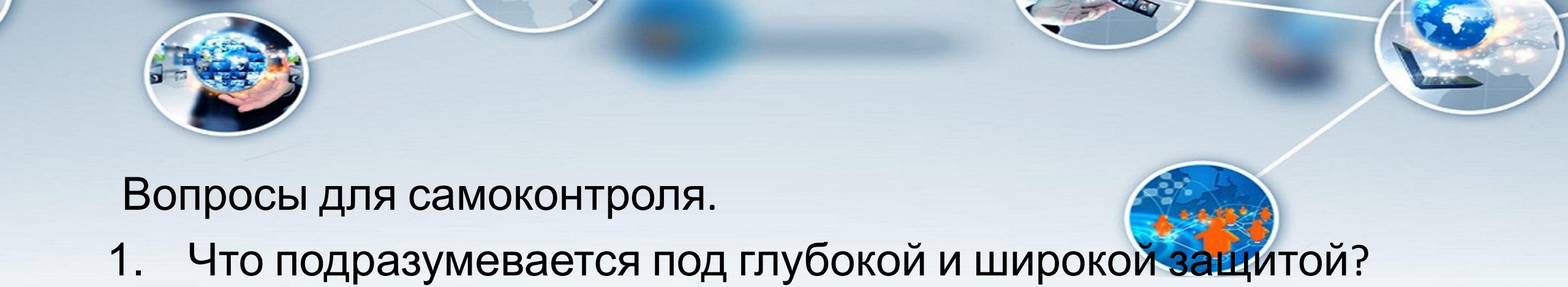
Профили администратора должны быть предоставлены только старшим должностным лицам, чтобы они могли контролировать настройку и отключение обычных профилей пользователей. Профили пользователей должны быть ограничены, чтобы разрешать использование компьютеров, рабочих станций или серверов только для тех целей, для которых они необходимы. Профили пользователей не должны позволять пользователю изменять системы или устанавливать и запускать новые программы.



Защита электронной почты и веб-браузера

Электронная почта между судном и берегом является жизненно важной частью работы судна. Соответствующая защита электронной почты и веб-браузера служит для:

- защиты берегового и бортового персонала от потенциальной социальной инженерии;
- предотвращения использования электронной почты как метода получения конфиденциальной информации;
- убедитесь, что обмен конфиденциальной информацией по электронной почте или по голосу надлежащим образом защищен для обеспечения конфиденциальности и целостности данных, например, защита с помощью шифрования.
- предотвращение выполнения вредоносных сценариев веб-браузерами и почтовыми клиентами.



Вопросы для самоконтроля.

1. Что подразумевается под глубокой и широкой защитой?
2. Что такое «границы доверия»?
3. Дайте объяснение термину «глубокоэшелонированная защита».
4. Чем отличаются технические и процедурные методы защиты?
5. В чём заключается ограничение и контроль сетевых портов, протоколов и сервисов?