Лекция 2. Информационная безопасность. Атрибуты кибербезопасности.

Что такое кибербезопасность? Кибербезопасность можно определить как «набор инструментов, политик, концепций безопасности, меры безопасности, руководящие принципы, подходы к управлению рисками, действия, обучение, лучшие практики, гарантии и технологии, которые могут быть использованы для защиты киберсреды и организации и активов пользователя.

Информационная безопасность. Атрибуты кибербезопасности

Киберсреда. В рамках этого определения «киберсреда» включает взаимосвязанные сети как ИТ, так и киберфизических систем, использующих электронные, компьютерные и беспроводные системы, включая информацию, услуги, социальные и бизнес-функции, которые существуют только в киберпространстве. На корабле компьютерные системы будут включать в себя ряд компонент информационных технологий (например, персональные компьютеры (ПК), ноутбуки, планшетные устройства, серверы и сетевые компоненты, такие как маршрутизаторы, коммутаторы и т. д.), и эксплуатационную технику (например, системы управления, датчики, исполнительные механизмы, радары и т. д.). «Активы организации и пользователя» включают подключенные вычислительные устройства, персонал, инфраструктуру, приложения, услуги, телекоммуникационные системы и совокупность передаваемых, обрабатываемых и / или хранимых данных и информации в киберсреде.

Кибербезопасность стремится достичь и поддерживать восемь общих целей безопасности

Конфиденциальность

Честность

Доступность (включая надёжность)

Полезность (Непрерывность судовых операций)

Безопасность (Безопасность людей & ресурсов)

Подлинность

Устойчивость

Владение

(или Control)

Контроль доступа к кораблю и корабельным операционным системам

Угрозы, которыми киберохрана стремится заняться

Мотивация кибератаки на судовую систему

(a) неправомерное использование киберпространства (кибер- злоупотребление)

(б) группы активистов

(c) шпионаж

(d) организованная преступность

(e) терроризм

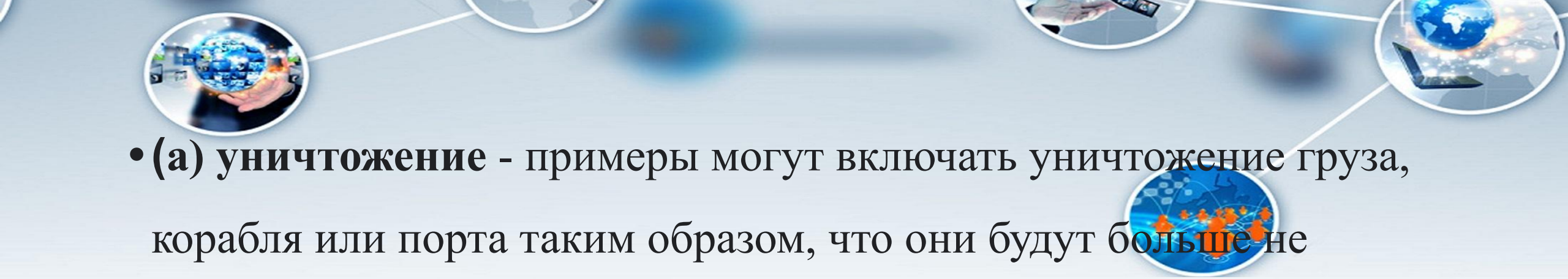
(f) война

Таким образом, субъекты угроз можно разделить на одну из категорий, которые подробно описаны далее:

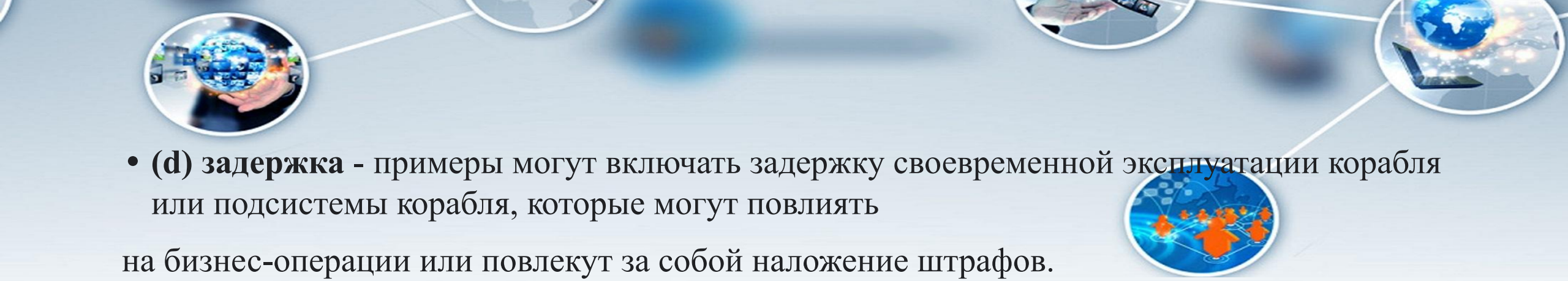
- (а) отдельные лица, например, «сценаристы» и инсайдеры;
- (б) группы активистов, также известные как «хактивисты»;
- (в) коммерческие конкуренты;
- (г) киберпреступники;
- (д) террористы;
- (е) национальные государства и субъекты, спонсируемые государством.

Каковы последствия того, что злоумышленники пытаются добиться?

Независимо от цели и мотивации нападения на корабль или флот, у субъектов угрозы будет результат, которого они пытаются достичь. Эти эффекты могут быть направлены на общий бизнес, корабль или подсистемы корабля и **сгруппированы в следующие категории**:



- **(а) уничтожение** - примеры могут включать уничтожение груза, корабля или порта таким образом, что они будут больше не пригодны для использования.
- **(б) ухудшение** - примеры могут включать влияние на скорость или маневренность корабля, способность точно ориентироваться или точно отслеживать местную среду до такой степени, что способность корабля работать значительно ухудшается.
- **(с) отказ** - примеры могут включать отказ в доступе к судовым системам или информации / данным, возможно, по таким



- **(d) задержка -** примеры могут включать задержку своевременной эксплуатации корабля или подсистемы корабля, которые могут повлиять

на бизнес-операции или повлекут за собой наложение штрафов.

- **(e) сдерживание -** примеры могут включать в себя влияние на бизнес от деятельности в определенных районах мирового океана, работающие на определенных рынках или имеющие доступ к конкретным портам с коммерческой точки зрения.
- **(f) обнаружение -** примеры могут включать обнаружение людей, груза или местоположения судов, и отслеживать такие случаи, когда запланированная физическая кража или манипуляции с грузом могут иметь место.
- **(g) отвлечение -** примеры включают способность изменять состояние датчика, чтобы обеспечить отвлечение во время извлечения данных / информации. Приведенные примеры не являются исчерпывающими, и соответствующие эффекты выбираются, учитывая лицо угрозы и мотивацию любой атаки.

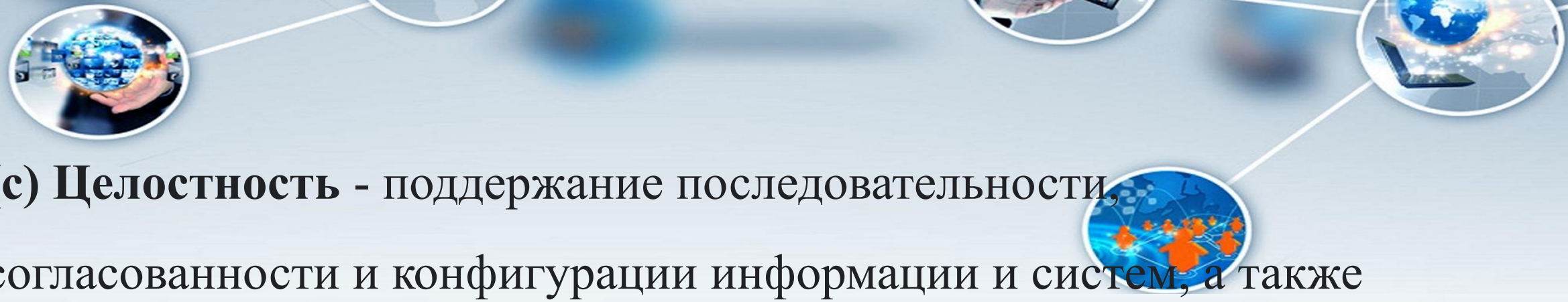
Атрибуты кибербезопасности

- Морская среда включает в себя множество технологий, как существующих, так и новых, и принятый подход к кибербезопасности будет варьироваться от судна к судну, в зависимости от сложности, владения, использования и цепочки поставок, поддерживающих проектирование, строительство, эксплуатацию и захват корабля. Поэтому вопросы кибербезопасности лучше всего решать с помощью рассмотрения набора атрибутов безопасности, что позволяет принимать соответствующие решения, в зависимости от характера киберфизической системы (например, корабль, высокоскоростной корабль или MODU) и потенциальных угроз.

Ключевые атрибуты кибербезопасности применительно к киберфизическим системам

а) Конфиденциальность - контроль доступа и предотвращение несанкционированного доступа для отправки данных, которые могут быть конфиденциальными по отдельности или в совокупности. Судовые системы и связанные с ними процессы должны быть спроектированы, внедрены, эксплуатироваться и поддерживаться таким образом, чтобы предотвратить несанкционированный доступ, например, к конфиденциальным финансовым, коммерческим или личным данным.

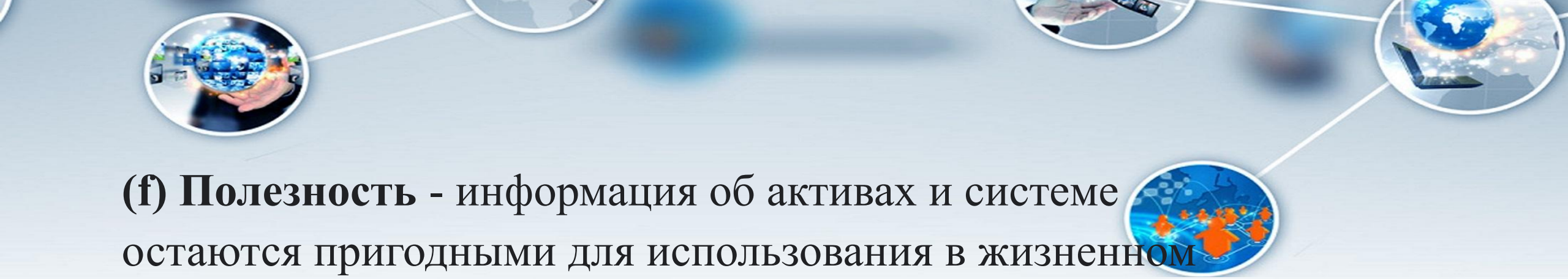
(b) Владение и / или контроль - разработка, реализация, функционирование и обслуживание судовых систем и связанных с ними процессов с целью предотвращения несанкционированного контроля, манипуляции или вмешательства. Судовые системы и связанные процессы должны быть спроектированы, внедрены, должны эксплуатироваться и поддерживаться, чтобы предотвратить несанкционированный контроль, манипуляции или вмешательство.



(c) Целостность - поддержание последовательности, согласованности и конфигурации информации и систем, а также предотвращение несанкционированных изменений в них. В судовых системах и связанных с ними процессах должны быть спроектированы, внедрены, эксплуатироваться и обслуживаться таким образом, чтобы предотвратить внесение несанкционированных изменений в активы, процессы, состояние системы или конфигурацию самой системы.

(d) Аутентичность - обеспечение того, чтобы входные и выходные данные судовых систем, систем и любых связанных процессов и данных о судне, являются подлинными и не были подделаны или изменены. Также должна быть возможность проверить подлинность компонентов, программного обеспечения и данных в системах и любых связанных процессах.

(e) Доступность (включая надежность) - обеспечение того, чтобы информация об активах, системах, и связанные процессы были постоянно доступны и могли использоваться в соответствующем и своевременном этапе. Для достижения требуемой доступности может потребоваться каждый из элементов, имеющий соответствующий и пропорциональный уровень устойчивости.



(f) Полезность - информация об активах и системе остаются пригодными для использования в жизненном цикле судового актива. Судовые системы и связанные с ними процессы должны быть спроектированы, внедрены, эксплуатироваться и обслуживаться таким образом, чтобы использование судовых активов поддерживалось на протяжении всего их жизненного цикла.

(g) Безопасность - проектирование, реализация, эксплуатация и техническое обслуживание судна, системы и связанных с ними процессов, чтобы предотвратить создание вредных состояний, которые могут привести к травмам или гибели людей, а также к непреднамеренному физическому или экологическому повреждению.


(h) Устойчивость - способность информации об активах и системах к преобразованию, своевременному обновлению и восстановлению в ответ на неблагоприятные события. Дизайн, внедрение, эксплуатация и обслуживание судовых систем и связанных с ними процессов должны быть такими, чтобы избежать каскадных отказов. В том случае, если система или связанный процесс страдают сбоями, повреждениями или отключениями, возникает проблема возможности восстановления нормального рабочего состояния или приемлемого состояния непрерывности бизнеса.

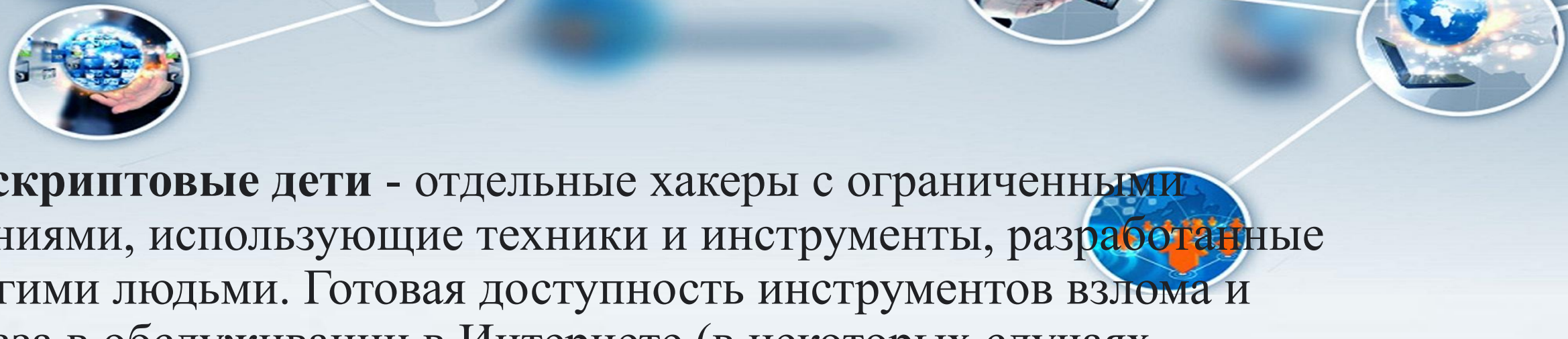
Группы субъектов угрозы

Серьезность и сложность угрозы будет определяться индивидуальными особенностями человека, например:

- **(а) халатный, неосторожный или невежественный сотрудник или подрядчик**, не соблюдающий приемлемое использование или другие политики безопасности, или из-за ошибки или упущения, может скомпрометировать систему безопасности.
- **(б) не злоумышленники**, которые не стремятся нанести вред системам или данным, но могут иметь доступ к системам без разрешения или ведома владельца и могут вызвать случайное повреждение.

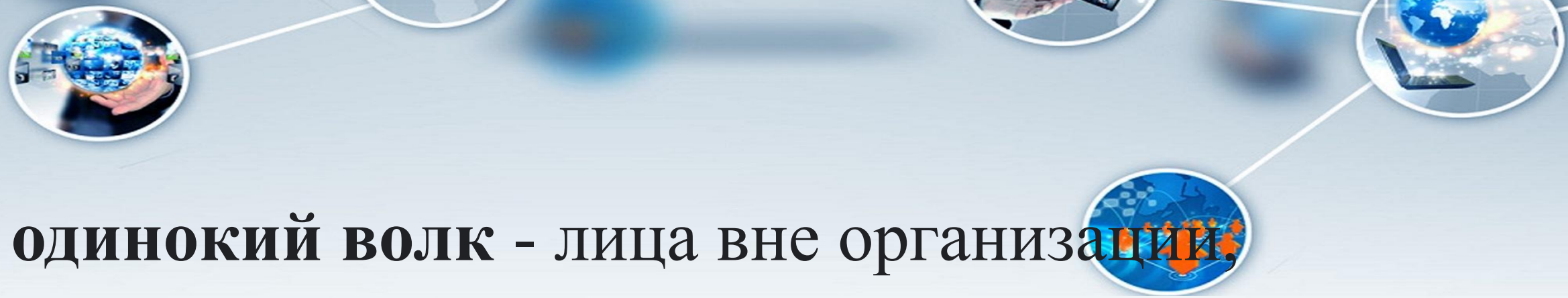
(c) недовольный сотрудник или подрядчик с ограниченными ИТ-навыками - мотивация может быть разной; намерение может заключаться в краже или утечке конфиденциальной информации, саботаже или нарушении операции с кораблем и т. д.

(d) недовольный сотрудник или подрядчик со значительными ИТ-навыками, включая системных администраторов - эти люди могут нанести значительный ущерб, особенно если они имеют доступ к широкому спектру систем с административными привилегиями. Они могут иметь достаточные знания и способность обходить средства контроля и защитные меры, и могут уметь удалять доказательства своей деятельности, например, удалять или измененять записи в системных журналах.



(e) скриптовые дети - отдельные хакеры с ограниченными знаниями, использующие техники и инструменты, разработанные другими людьми. Готовая доступность инструментов взлома и отказа в обслуживании в Интернете (в некоторых случаях распространяются в технических журналах) означает, что уровень технического понимания, необходимый для количества запусков атаки было значительно сокращен.

(f) кибервандалы - эта группа может быть очень хорошо осведомленной и может развиваться или дополнительно расширить собственные инструменты. Их мотивы не являются ни финансовыми, ни идеологическими - они взламывают или разрабатывают вредоносное ПО, потому что могут и хотят показать, на что они способны.



(g) одинокий волк - лица вне организации, обладающие продвинутыми техническими знаниями. Эта группа может уметь удалять свидетельства своей деятельности, например, удаление или изменение записей в системных журналах. Они также могут иметь достаточные знания и умение обходить средства контроля и защитные меры.



Вопросы для самоконтроля

1. Перечислите возможные цели кибератак на судовую систему.
2. Перечислите категории объектов киберугроз.
3. Перечислите возможные последствия кибератак.
4. Перечислите атрибуты кибербезопасности.