Лекция 2. CIA Triad: конфиденциальность, целостность, доступность

Цель лекции: Ознакомить студентов с основной триадой информационной безопасности и дать объяснения моделям безопасности.

План лекции:
1. Понятие информационной безопасности
2. Субъекты информационных отношений
3. Модели безопасности

Понятие информационной безопасности

Информационная безопасность (англ. *Information Security*, а также — англ. *InfoSec*) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая).

Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации.

Рисунок 1 Системное понимание информационной безопасности

Объектами опасного информационного воздействия и, следовательно, ИБ могут быть сознание, психика людей, информационно-технические системы различного масштаба и назначения.

Субъектами ИБ следует считать те органы и структуры, которые занимаются ее обеспечением.

Средства обеспечения ИБ – это средства с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации и т.д.

Принципы ИБ: законность, баланс интересов личности, общества и государства, комплексность, системность, интеграция с международными системами безопасности, экономическая эффективность и т.д.

Объекты защиты информации:

- Владельцы и пользователи
- Носители и средства обработки
- Системы связи и информатизации
- Объекты органов управления

Субъекты информационных отношений:

- Общественные или коммерческие организации и предприятия (юридические лица)
- Государство (в целом или отдельные его ведомства, органы и организации)
- Отдельные граждане (физические лица)

Будучи заинтересованным хотя бы в одном из вышеуказанных свойств, субъект информационных отношений:

- является *УЯЗВИМЫМ;*
- Потенциально подвержен *УЩЕРБУ* (прямому или косвенному, моральному или материальному);
- Заинтересован в своей *ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.*

Модели безопасности

Понятие информационной безопасности может быть пояснено с помощью так называемых моделей безопасности.

Суть этих моделей заключается в следующем: множество всех видов нарушений безопасности делится на несколько базовых групп таким образом, чтобы любое возможное нарушение обязательно можно было отнести по

крайней мере к одной из этих групп. Затем система объявляется безопасной, если она способна противостоять каждой из этих групп нарушений.

Триада "конфиденциальность, целостность, доступность"

Впервые этот принцип был изложен в статье "Защита информации в компьютерных системах", написанной Зальцером и Шредером в 1975-м году и опубликованной в "Communications of the ACM".

Авторы постулировали, что все возможные нарушения информационной безопасности всегда могут быть отнесены по меньшей мере к одной из трех групп: нарушения конфиденциальности, нарушения целостности или нарушения доступности.

Рисунок 2 Триада "конфиденциальность, целостность, доступность"

Конфиденциальность. Меры, предпринимаемые для обеспечения конфиденциальности, предназначены для предотвращения попадания конфиденциальной информации не тем людям, при этом гарантируя, что нужные люди действительно могут ее получить: доступ должен быть ограничен теми, кто уполномочен просматривать рассматриваемые данные. Также обычно классифицируют данные в соответствии с количеством и типом ущерба, который может быть нанесен, если они попадут в непреднамеренные руки. В соответствии с этими категориями могут быть приняты более или менее строгие меры.

Целостность. Целостность подразумевает поддержание согласованности, точности и достоверности данных в течение всего их жизненного цикла. Данные не должны быть изменены при транспортировке, и должны быть предприняты шаги, чтобы гарантировать, что данные не могут быть изменены посторонними лицами (например, в нарушение конфиденциальности). Эти меры включают в себя права доступа к файлам и контроль доступа пользователей.

Доступность. Доступность лучше всего обеспечивается тщательным обслуживанием всего оборудования, немедленным выполнением ремонта оборудования, когда это необходимо, и поддержанием правильно функционирующей среды операционной системы, свободной от конфликтов программного обеспечения. Также важно быть в курсе всех необходимых обновлений системы. Обеспечение адекватной пропускной способности связи и предотвращение возникновения узких мест одинаково важны. Избыточность, отказоустойчивость, RAID и даже кластеры высокой доступности могут смягчить серьезные последствия, когда проблемы с оборудованием возникают.

Список свойств безопасной системы следует расширить, добавив к КЦД еще одно свойство — «неотказуемость».

Неотказуемость (non-repudiation) — это такое состояние системы, при котором обеспечивается невозможность отрицания пользователем, выполнившим какие-либо действия, факта их выполнения, в частности отрицания отправителем информации факта ее отправления и/или отрицания получателем информации факта ее получения.

ФСБ в своей методичке по персональным данным, указав триаду как основные характеристики безопасности, добавила еще: "*в дополнение к перечисленным выше основным характеристикам безопасности могут рассматриваться также и другие характеристики безопасности. В частности, к таким характеристикам относятся неотказуемость, учетность (иногда в качестве синонима используется термин «подконтрольность»), аутентичность (иногда в качестве синонима используется термин «достоверность») и адекватность*". А в 91-м Джон МакКамбер предложил свою модель на базе триады, названную им моделью информационной безопасности МакКамбера.

ОЭСР в 1992-м году предложила свои 9 принципов безопасности - Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management и Reassessment.

Гексада Паркера

Одной из наиболее популярных альтернатив триаде КЦД является так называемая гексада Паркера (Parkerian Hexad) (Дон Паркер предложил свою гексаду в работе «Fighting Computer Crime» (1998)), в которой определено шесть

базовых видов нарушений, в число которых, помимо нарушений конфиденциальности, доступности и целостности, входят еще три вида нарушений: владение или контроль (possession или control), аутентичность (достоверность) и полезность (utility).

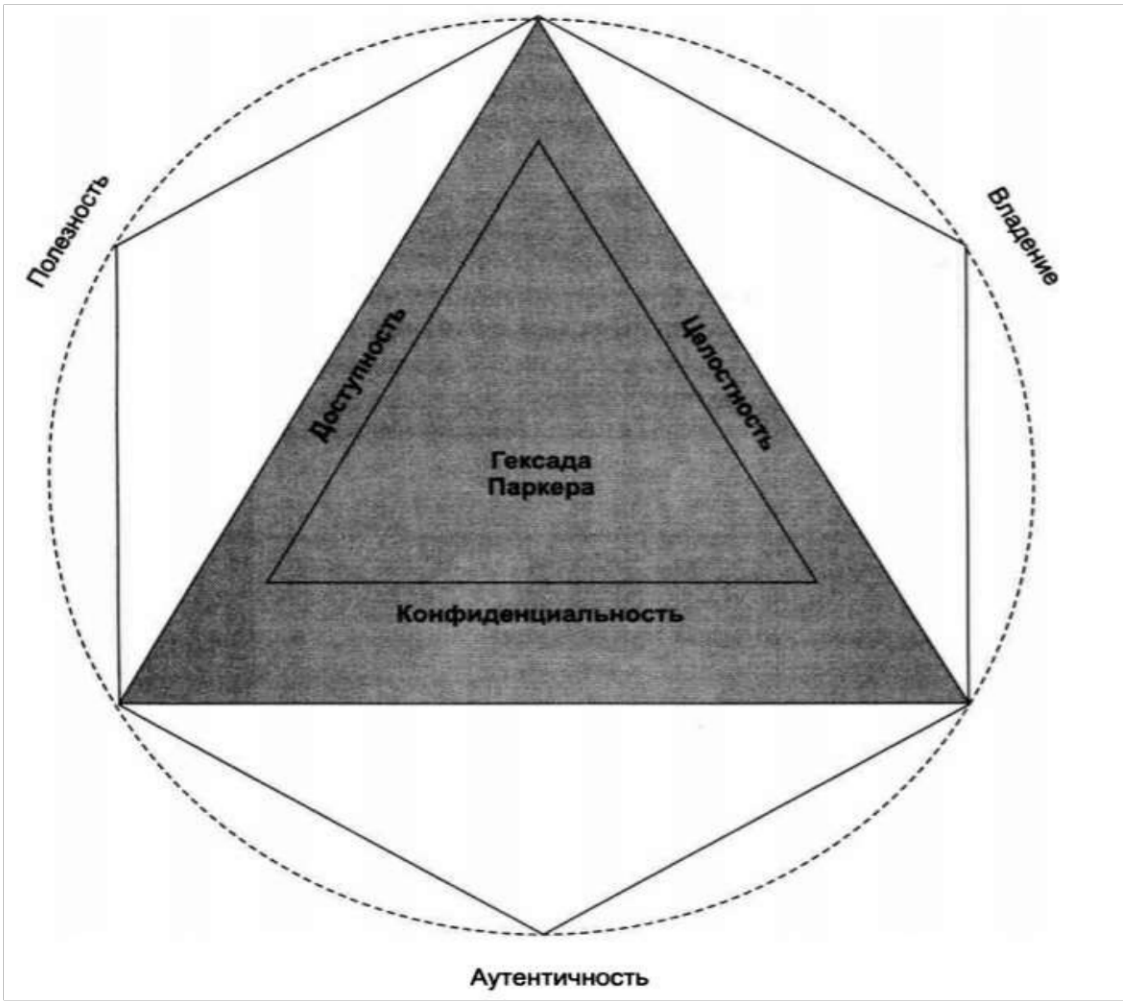

Рисунок 3 Гексада Паркера

Аутентичность (authenticity) — это состояние системы, при котором пользователь не может выдать себя за другого, а документ всегда имеет достоверную информацию о его источнике (авторе). Из этого определения видно, что аутентичность является аналогом неотказуемости

Владение (possession) — это состояние системы, при котором физический контроль над устройством или другой средой хранения информации предоставляется только тем, кто имеет на это право

Полезность (utility) — это такое состояние ИС, при котором обеспечивается удобство практического использования как собственно информации, так и связанных с ее обработкой и поддержкой процедур. В безопасной системе меры, предпринимаемые для защиты системы, не должны

неприемлемо усложнять работу сотрудников, иначе они будут воспринимать их как помеху и пытаться при всякой возможности их обойти.

Владение/контроль: вор украл у вас запечатанный конверт с банковскими картами и PIN-кодами к ним. Даже если вор не открыл этот конверт и не нарушил тем самым его конфиденциальность, это все равно должно вызывать беспокойство владельца конверта, который потерял над ним контроль.

Полезность: Допустим вы зашифровали свой жесткий диск и забыли пароль (ключ). Для данных на диске сохраняется конфиденциальность, целостность, доступность, достоверность и контроль, но... вы не можете ими воспользоваться. Это и есть нарушение полезности.

Модель STRIDE

Еще одним вариантом определения безопасности ИС является модель STRIDE (аббревиатура от англоязычных названий типов нарушений безопасности, перечисленных ниже). В соответствии с этой моделью ИС находится в безопасности, если она защищена от следующих типов нарушений: подмены данных, изменения, отказа от ответственности, разглашения сведений, отказа в обслуживании, захвата привилегий.

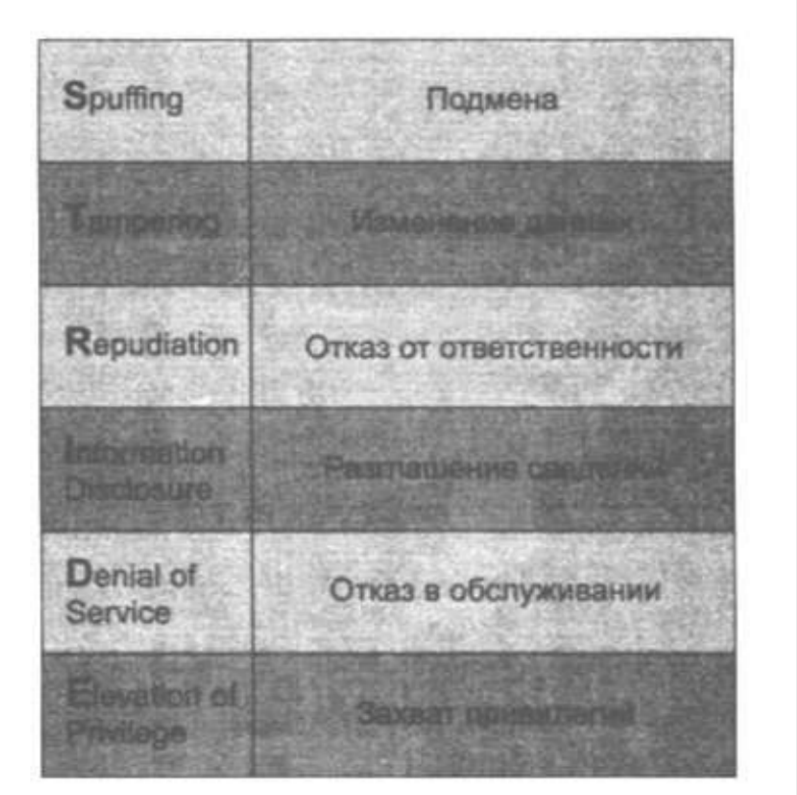

Рисунок 4 Модель STRIDE

Подмена данных (spoofing) — это такое нарушение, при котором пользователь или другой субъект ИС путем подмены данных, например IP-

адреса отправителя, успешно выдает себя за другого, получая таким образом возможность нанесения вреда системе.

Изменение (tampering) означает нарушение целостности.

Отказ от ответственности (repudiation) представляет собой негативную форму уже рассмотренного нами свойства неотказуемости (non-repudiation).

Разглашение сведений (information disclosure) — это нарушение конфиденциальности.

Отказ в обслуживании (denial of service) касается нарушения доступности.

Захват привилегий (elevation of privilege) заключается в том, что пользователь или другой субъект ИС несанкционированным образом повышает свои полномочия в системе, в частности незаконное присвоение злоумышленником прав сетевого администратора снимает практически все защитные барьеры на его пути.

Модель STRIDE используется компанией Microsoft при разработке безопасного программного обеспечения.

Большие данные ставят дополнительные задачи перед парадигмой ЦРУ из-за огромного объема информации, которую необходимо защищать, множества источников, из которых они поступают, и разнообразия форматов, в которых они существуют. Повторяющиеся наборы данных и планы аварийного восстановления могут увеличить и без того высокие затраты. Кроме того, поскольку основной задачей больших данных является сбор и предоставление какой-либо полезной интерпретации всей этой информации, часто отсутствует ответственный надзор за данными.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.

2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.

3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.

4. Башлы П. Н. Информационная безопасность [Электронный учебник] : учебное пособие / Башлы П. Н.. - Евразийский открытый институт, 2012. - 311 c. - Режим доступа: http://iprbookshop.ru/10677