САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

Введение в специальность

Доцент каф. ГИиИБ, к.т.н.
Копенков Василий Николаевич
vkop@geosamara.ru

Научный корпус (№18), к. 701.

Основы информационной безопасности.

Словосочетание "информационная безопасность" – что означает? А «Защита информации»?

В Доктрине информационной безопасности РФ – «состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства»

Общее определение: «Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести **неприемлемый** ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры».

Взаимосвязи.

Защита информации – это *комплекс мероприятий*, направленных на обеспечение информационной безопасности.

Выводы по определениям.

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. (Универ, ЦСКБ, …)

2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие.

Определение ИБ - "ущерб" – «неприемлемый»?

Люди, оборудование, информация, деньги?

Почему ИБАС?

Термины "безопасность информации" vs "защита информации".

Термин "безопасность" включает в себя не только понятие защиты, но также и **аутентификацию**, аудит, обнаружение проникновения в ИС и т.д.

Поэтому «ИБ», а на «ЗИ» – курс, специальность и более широкое направление деятельности.

Проблемы и их характеристики.

1. Фирма имеет несколько офисов, расположенных на большом расстоянии друг от друга.
2. Сетевой администратор осуществляет удаленное управление компьютером.
3. Пользователь несанкционированно получает доступ к удаленному компьютеру с правами законного пользователя, либо, имея право доступа к компьютеру, получает доступ с гораздо большими правами.
4. Фирма открывает свой сайт в Internet.
5. 6. 7. …

Для решения:

1) Формальные критерии, которым должны соответствовать защищаемые информационные технологии
2) практический аспект – конкретный комплекс мер безопасности.

На практике:

Вопросы:

Где уязвимые места в информационной системе?
Какие угрозы безопасности существуют, как оценить их серьезность?
Какой остаточный уровень рисков допустим?
Какой комплекс мер снизит риски до допустимого уровня?

Ответы: … «Ну,… это, … вообщем, админ разберется… Наверное…»

Основные составляющие ИБ.

Доступность – возможность за приемлемое время получить требуемую информационную услугу.

Под **целостностью** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – защита от несанкционированного доступа к информации.
(*Важность и ценность …*)

Что первое? Или главное? Почему?

Что и когда важно?

Где здесь место термину «неприемлемый»? И в каком качестве?

Важность и ценность.

До компьютеров – что с информацией?

В период персоналок – индивидуальная защита.

С появлением интернета и сетей – *от чего и как защищаться?*

С появлением различных сервисов и распределенных приложений – *защищаться или работать?*

Электронный документ-оборот – *удобство и ускорение или очередные проблемы?*

Мульти-сервисные службы и кросс-платформенные приложения – *что с этим делать?*

Очень старые новости – за 10 лет до вашего рождения ☺
-По распоряжению президента США Клинтона (от 15 июля 1996 года) была создана Комиссия по защите критически важной инфраструктуры как от физических нападений, так и от атак, предпринятых с помощью информационного оружия!!!
-Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (июль 1998) - побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения.
-Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России.
-Начиная с 1996 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей.
-В марте 1999 года был опубликован 4 годовой отчет "Компьютерная преступность и безопасность-1999: проблемы и тенденции" (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). В отчете отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками; атакам через Internet подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос "были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?" ответили "не знаю".
-и т.д.

Жизненный цикл.

1) Системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды, порой прощупывание уязвимых мест ведется медленно и растягивается на часы/дни/недели, так что подозрительная активность практически незаметна.

2) Современные технологии программирования не позволяет создавать безошибочные программы (включая ОС), что не способствует быстрому развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные средства обеспечения ИБ с привлечением ненадежных компонентов (программ).

- *Инициация/Решение – …*
- *Выбор/Закупка – …*
- *Установка/Настройка – …*
- *Эксплуатация – …*
- *Вывод из эксплуатации – …*

Люди, дома, механизмы,
оборудование, ПО, системы,
сервисы, компоненты,
должности, роли, и … все-все-все …

Что еще?

ООП - О необходимости объектно-ориентированного подхода к информационной безопасности

-*Большие системы*
-*Программирование*
-*Проектирование*
-*Разработка*
-*Контроль*

СЛОЖНОСТЬ!!! (ПО, Доки (нормативка), Требования, Правила, и пр.)

"devide et impera"? как делить-то?

Класс – что это?
Объект? Контейнер? Компонент?

Активность объектов.

инкапсуляция наследование полиморфизм

Какие ужасные слова, а мы не планируем/не хотим программировать!!!

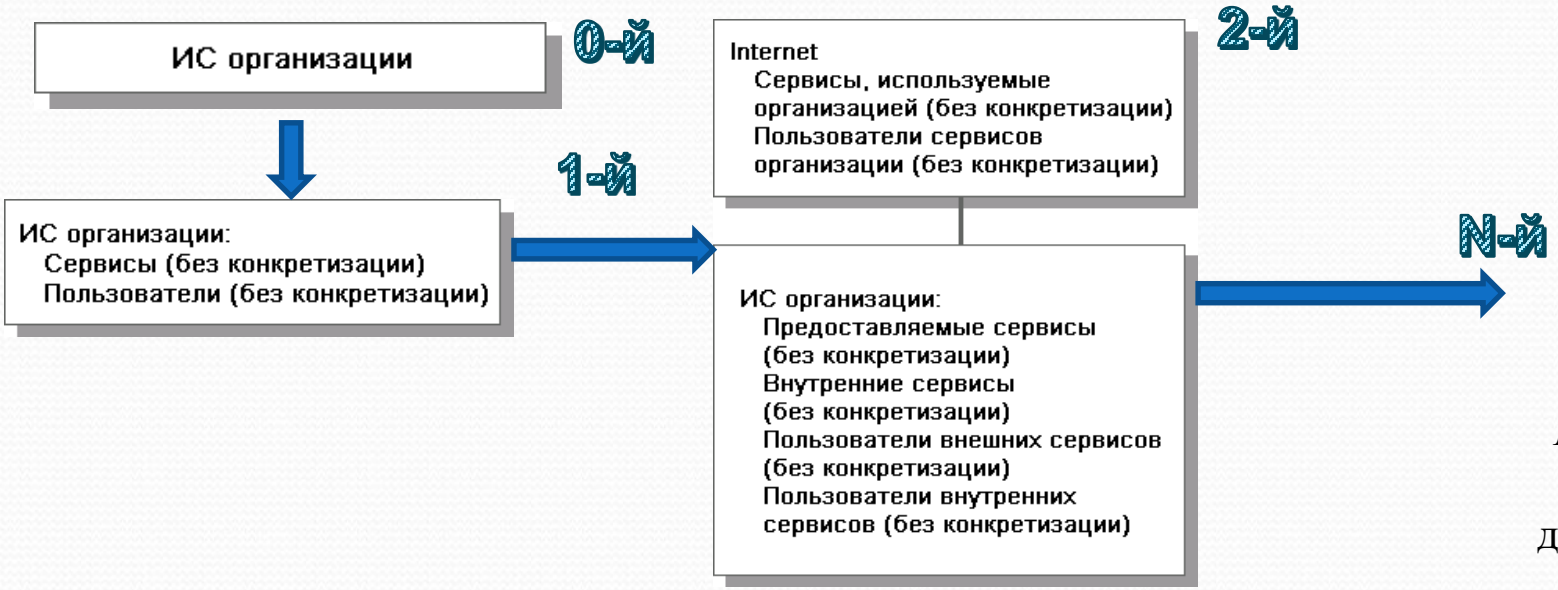
ООП – подробности.

Объекты реального мира

Грани – Доступность, Целостность, Конфиденциальность

Еще грани/ УРОВНИ ***3x4=12***
– Законодательный,
– Административный
– Процедурный
– Программно-технический.

Уровни детализации? 0 – атомарный.



Карта ИС.

детализация?

Общие принципы работы с Информацией.

Собственник …
Множество
информационных ценностей

Атаки …

Противники или **оппоненты**,

Уязвимости …
(потеря **конфиденциальности**),
(потеря **целостности**)
(потеря **доступности**).

Контрмеры …

Риски …

политика безопасности
механизмы и сервисы безопасности.

Классификация сетевых атак.

I. *Пассивная атака*

II. *Активные атаки*

- **Отказ в обслуживании - DoS-атака**

- **Модификация потока данных - атака «man in the middle»**

- **Создание ложного потока (фальсификация)**

- **Повторное использование (replay-атака)**

Общая модель сетевого взаимодействия.

Механизмы:

- ***Алгоритмы симметричного шифрования.***
- ***Алгоритмы асимметричного шифрования.***
- ***Хэш-функции и ЭЦП.***

Сервисы:

Конфиденциальность – предотвращение пассивных атак для передаваемых или хранимых данных.

Аутентификация – подтверждение того, что информация получена из законного источника, и получатель действительно является тем, за кого себя выдает.

Целостность – сервис, гарантирующий, что информация при хранении или передаче не изменилась.

Невозможность отказа – невозможность, как для получателя, так и для отправителя, отказаться от факта передачи.

Контроль доступа – возможность ограничить и контролировать доступ к системам и приложениям по коммуникационным линиям.

Доступность – сервис предназначен для того, чтобы минимизировать возможность осуществления **DoS-атак.**

Модель безопасности ИС.

Два типа атак:

1. Доступ к информации с целью получения или модификации хранящихся в системе данных.
2. Атака на сервисы, чтобы помешать использовать их.

Сервисы безопасности, которые предотвращают нежелательный доступ, можно разбить на две категории: *Первая категория* определяется в терминах сторожевой функции. Эти механизмы включают процедуры входа. *Вторая линия обороны* состоит из различных внутренних мониторов, контролирующих доступ и анализирующих деятельность пользователей.

Одним из основных понятий при обеспечении безопасности информационной системы является понятие ***авторизации*** - определение и предоставление прав доступа к конкретным ресурсам и/или объектам.

Угрозы.

Угроза – это *потенциальная* возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку – злоумышленником.

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**.

Для большинства уязвимых мест окно опасности существует сравнительно долго, поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Угрозы по типам.

Доступность – .

- отказ пользователей;
- внутренний отказ ИС;
- *отказ поддерживающей инфраструктуры.*

… "обиженные" сотрудники ☺

Вредоносное программное обеспечение: Описание, Функции, Вирусы, Черви, Троянцы, Макровирусы, Активное содержимое …

Целостность – .

- Кто? Что делает? *Результат…*
- Электронное противостояние
- Динамическая целостность

Конфиденциальность –

- Предметная и служебная информация.
- Полномочия и замены.
- Выставки и пр.