ФГАОУ ВО «Санкт-Петербургский политехнический университет»

ПОДХОД К ПОСТРОЕНИЮ ОБОБЩЕННОЙ МОДЕЛИ КИБЕРБЕЗОПАСНОСТИ

доктор технических наук, профессор, П. Д. Зегжда

Раздел 1.
Эволюция технологий защиты

Время - величайший из новаторов

Роджер Бэкон

Предпосылки появления новой парадигмы информационной безопасности

1. • Рост числа компьютерных атак на системы управления критическими технологиями (Stuxnet, Flame, Duqu, Gauss, Red October, NetTraveler), кражи банковских активов, вывод из строя энергосистем, объектов ядерной промышленности.
2. • Рост эффективности средств разрушающего информационного воздействия как следствие увеличения возможностей информационных систем.
3. • Объектом атаки все чаще становятся не данные, а среда их обработки и системы управления реальными промышленными объектами и инфраструктурой.
4. • Атаки становятся все более тщательно подготовленными, а производство средств их осуществления превратилось в специфическую, но вполне легальную IT-отрасль
5. • Переход от шкалы уровней безопасности к оценке устойчивости систем и определению допустимого риска

Актуальные задачи обеспечения безопасности

- **Мониторинг и управление безопасностью в распределенных сетях, исследование уязвимостей как новый подход к оценке уровня безопасности.**
- **Интеграция зарубежных информационных технологий и отечественных средств защиты.**
- **Развитие технологии виртуализации как мощного механизма защиты распределенных систем:**
  - **защита собственных средств виртуализации (доверенный гипервизор);**
  - **построение защищенных платформ с использованием технологии виртуализации.**
- **Интеграция средств сетевой защиты и вычислительных кластеров.**
- **Развитие поисковых исследований в части создания моделей политики безопасности систем с размытым периметром и «некорпоративных» систем и средств контроля и управления безопасностью в таких системах.**

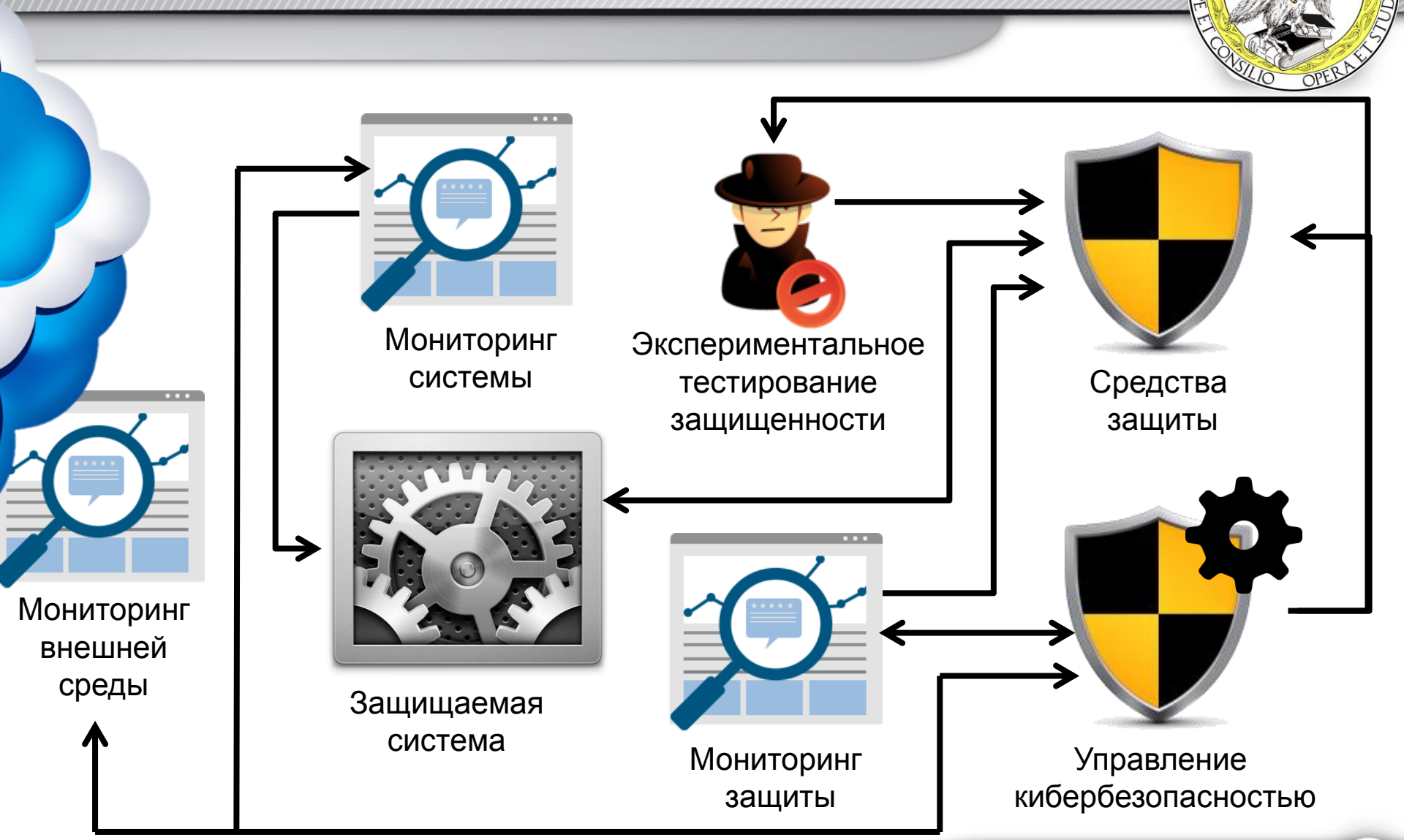
Эволюция парадигм защиты

	Полнота знаний о нарушителе	Полнота защиты	Уровень автома-тизации атаки	Анализ состояния системы	Технология защиты
Защита от НСД	Знание о полном множестве угроз с целью формирования моделей угроз и нарушителя	Устранение всех угроз, описанных в моделях угроз и нарушителя	Из типового набора	Отсутст-вует	Статичес-кая
Управление рисками	Оценка последствий реализации полного множества угроз	Для минимизации рисков предполагается устранение угроз с заданной вероятностью	Из типового набора	Неполный	Статичес-кая
Апостериор-ная защита	Не предполагается полноты знаний о множестве угроз	Полнота контроля за поведением системы и регистрация любой активности	Частичный	Неполный	Активная + адаптивная
Обеспечение кибербезо-пасности	Исследование не только защищаемой системы и механизмов реализации угроз, но и перспективных средств нарушения безопасности	Осуществляется противодействие существующим и перспективным средствам реализации угроз	Значительный	Полный	Динамичес-кая

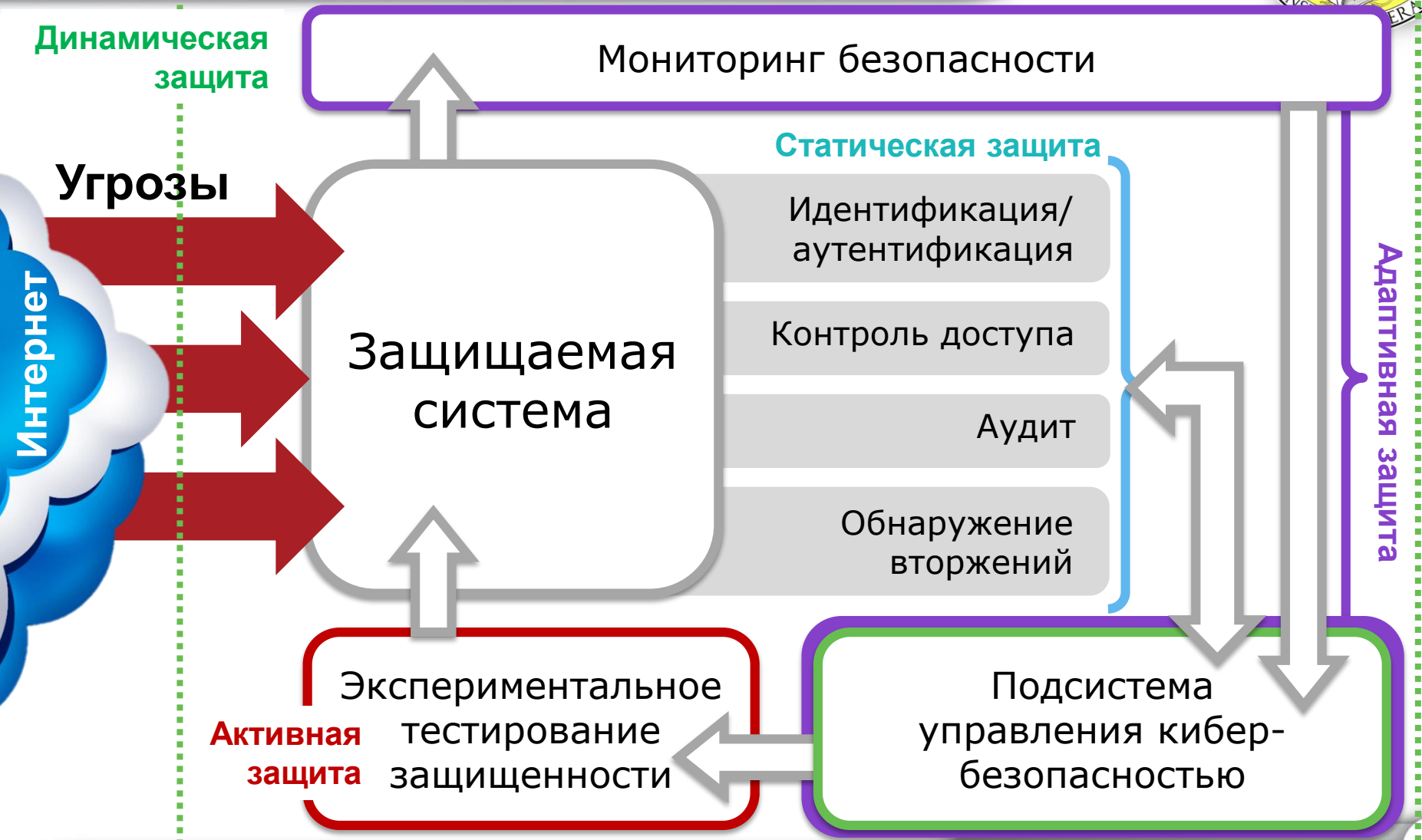
Эволюция технологий защиты

Характер защиты	Объекты мониторинга			Методы оценки безопасности	Основные характе-ристики
	Состояние системы	Состояние системы защиты	Обмен с окружающей средой		
Статическая	отсутствует	отсутствует	частичный	оценка по нормативным документам	Адекватность угрозам
Активная	частичный	отсутствует	анализ входящей информации	анализ информационной среды	Надёжность анализа входящей информации
Адаптивная	частичный	частичный	анализ входящей информации	контроль состояния средств защиты	Толерантность к угрозам, устойчивость управления
Динамическая	полный	полный	анализ входящей информации и каналов связи	мониторинг безопасности системы, оценка рисков	Инвариантность защиты, достаточность, устойчивость к уязвимостям

Структурная схема системы обеспечения кибербезопасности



Функциональная схема построения систем защиты



Раздел 2. Феноменологический подход к моделированию безопасности

Мысль должна быть направлена на необъятное

Марсилио Фичино

Цель исследования

Создание автоматизированной системы решения задач обоснования выбора функций защиты, адекватных функциям деструктивных воздействий на крупномасштабные гетерогенные компьютерные системы

Релевантные подходы к экспериментальному анализу систем защиты

- Сканирование защищенности (Nessus, xSpider, MaxPatrol)
- Моделирование контрмер
- Топологический анализ уязвимостей
- Имитационное моделирование
- **Функциональное моделирование (модели Хартстона (пятимерное пространство безопасности), Адепт, …)**

Представление системы

$$H =< I, C_1, C_2, \ldots, Cn, \Gamma >$$

I	• множество информационных единиц
$C_1, C_2, \ldots, C_n$	• множество типов связей между информационными элементами
Γ	• отображение, задающее связи из принятого набора между информационными единицами

Представление всех сущностей системы (и тех, которые отвечают за реализацию основного информационного процесса КС, и отвечающих за управление и организацию защиты)

Функциональная модель нарушений безопасности

Состояние безопасности системы на каждом уровне иерархии $< O, R, Rul, L_{ij} >$

O	• множество допустимых объектов $\{O_i\}$
R	• множество отношений, построенное по бинарному принципу, тип отношений $\{R_{ij}\}$ определен для типа объекта
Rul	• правила контроля цепочки отношений в соответствии с политикой безопасности. Цепочки отношений строятся с использованием объектного подхода с использованием принципов наследования, инкапсуляции, полиморфизма.
L_{ij}	• функции передачи от объекта к объекту, построенные на типе отношений и включают: запись, чтение, изменение и т.д.

Описание функционирования системы

Построение цепочки $R \times R$ с инициализацией функции L_{ij}, что приводит к действиям над объектом O или изменению отношений $\{O_i\}$

Изменение состояния системы

Реализация отношений R_i

Изменение множества $\{O_i\}$

Функции безопасности (идентификация O_i, аутентификация $O_i R O_j$, фильтрация по параметрам, криптографические преобразования $O_i \xrightarrow[M_k]{} O^k$)

Функции L_{ij}

Функции, не изменяющие объект, что сохраняет $\{O_i\}$, но может привести к нарушениям Rul

Функции, изменяющие объект L^{new}, что приводит к изменению $\{O_i\}$

Информационный поток F – последовательность парных отношений узлов в соответствии с назначением системы

Систематизация функциональных типов нарушений безопасности [1]

Создание нового объекта, не входящего в допустимое множество объектов *O* или путем изменения параметров (отношений) свойственных существующим объектам. При данном механизме возникают следующие частные случаи:

Утверждение 1.1. Создание «деструктивного» объекта, что представляет собой реализованную *атаку*.

Утверждение 1.2. Возможное превышение заданной скорости создания «правильных» объектов, что приводит к отказу в обслуживании. Изменение параметров объекта или параметров функции его преобразования, называется *уязвимостью.*

Систематизация функциональных типов нарушений безопасности [2]

Изменение функций, построенных на типе отношений.

1. Целенаправленное изменение функций L_{ij} – следствие появления новых объектов (как правило, это направлено на нарушение функций защиты и является механизмом атаки).
2. Не контролируемое, но стабильное изменение L_{ij} вследствие наличия уязвимости
3. Целенаправленное использование уязвимости, что является механизмом атаки

Функциональная модель защиты

U – множество лиц-участников информационного процесса (потенциальных пользователей компьютерной системы), осуществляющих доступ к информации и ее обработку и обменивающихся информацией.

I – множество информационных объектов-контейнеров(документов, книг, папок, файлов и т. д.), хранящих информацию. Информация не может существовать сама по себе — она хранится в каком-либо контейнере.

Виды потоков:

$F^W \subseteq U \times I$ – отношение, описывающее потоки от пользователей к контейнерам;

$F^R \subseteq I \times U$ – отношение, описывающее потоки от контейнеров к пользователям.

Функциональная модель защиты: аксиомы безопасности

1. Для каждой информации существует по крайней мере один пользователь являющийся ее *доверенным источником*. Доверенные источники описываются функцией TrustSrc : I→U.
2. Для каждого пользователя известен набор информации, для которой он является уполномоченным потребителем. Эти полномочия описываются функцией Authority:U→I.

В каждый момент времени распределение информации в системе характеризуется следующими отношениями между пользователями и информацией:

1. Know $\subseteq$ U×I – отношение известности, которое определяет какой пользователь знает какую информацию.
2. Create $\subseteq$ U×I – отношение порождения, которое определяет какой пользователь поставляет какую информацию.

Функциональные критерии безопасности

Критерий безопасности состояния

1. Отношение известности не противоречит функции авторизации Know $\subseteq$ Authority.
2. Отношения порождения не противоречит функции доверенного источника Create $\subseteq$ TrustSrc.

Критерий безопасности для системы

1. Текущее состояние системы безопасно.
2. Транзитивное замыкание отношений Know и Create не противоречит аксиомам безопасности.

Функциональное моделирование

В самом общем виде механизм атаки и механизм защиты на функциональном уровне задан формальной моделью (изменение структуры и состав узлов).

Необходимо задать сценарий атаки

С созданием ложного узла (создание ложного узла и его описание в формате всех остальных узлов и дополнительная характеристика – вероятность обнаружения и удаления)

Без создания ложного узла на нарушении связи – нарушение совместимости и изменение функций рабочих узлов.

Процесс атаки – построение неконтролируемого маршрута на графе системы, который приводит к воздействию на критический ресурс.

Отличительные особенности предлагаемого подхода

1. Представление защиты и деструктивного воздействия набором функций по поддержанию или искажению информационных потоков в системе
2. Возможность построения полной группы событий нарушений безопасности
3. Возможность последующей конструкторской конкретизации и переход на параметрические модели

Определение киберпространства

Киберпространство – глобальная сфера в информационном пространстве, представляющая собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры.

«Глобальная сфера (домен) внутри информационного пространства, представляющая собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры». *(«Операции в киберпространстве», МО США, 2010 год).*

Киберпространство и кибербезопасность

КИБЕРПРОСТРАНСТВО

Виртуальная информационно-коммуникационная технологическая среда, образованная взаимосвязанными компонентами обеспечения **ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И УПРАВЛЕНИЯ ИМИ**

Киберпространство включает:

- **субъекты**: пользователи, администраторы, обслуживающий персонал, операторы систем и их абстрактные сущности (учетные записи, маркеры доступа и т.п.) в информационных системах
- **объекты**, включая **РЕСУРСЫ И ИНФОРМАЦИОННЫЕ АКТИВЫ**:
  - **компоненты среды передачи информации**: глобальные и локальные компьютерные сети, включая сеть Интернет, мультипротокольное сетевое оборудование, средства коммуникаций
  - **активные компоненты среды обработки и хранения информации**: мобильные системы, операционные системы и системы управления базами данных, платформы сетевых хранилищ данных и виртуализированных систем (виртуальные, облачные и грид-системы), а также компоненты их инфраструктуры и поддержки
  - **компоненты управляющих, технологических и исполнительных систем**: автоматизированные системы управления технологическими процессами (АСУ ТП), ERP-системы
  - **информационные ресурсы и хранилища данных**, к которым осуществляется доступ любого вида
- **системы защиты информации и управления информационной безопасностью**
- все возможные **взаимосвязи и взаимодействия**, устанавливаемые между ними в процессе деятельности

КИБЕРБЕЗОПАСНОСТЬ

Комплекс мер, направленных на достижение **ГАРАНТИРОВАННОГО** состояния **независимости киберпространства** от ущерба вследствие нарушений в его функционировании

Задачи кибербезопасности

АНАЛИЗ

механизмов нарушения защиты киберпространства, моделирование разрушающих воздействий

УПРАВЛЕНИЕ

кибербезопасностью, определение зоны устойчивости объектов защиты, анализ киберрисков, разработка стандартов и нормативов безопасности киберпространства

КИБЕРБЕЗОПАСНОСТЬ

СИНТЕЗ

средств защиты киберпространства

КОНТРОЛЬ

текущего состояния и функционирования компонентов киберпространства

Актуальные компоненты системы обеспечения кибербезопасности

- Использование динамической защиты в качестве средства активного противодействия
- Дополнительный контур защиты и проверка безопасности систем мониторинга
- Создание доверенной среды на основе виртуализации
- Удаленный контроль защищенности систем управления исполнительными механизмами
- Использование доверенной сети Интернет
- Создание ложных объектов нападения для критических систем
- Применение систем активной удаленной проверки работы (автотестирование)

Раздел 3.
Язык описания безопасности компьютерных систем

Так как вы не можете сделать все, что хотите,
то желайте только того, что можете сделать

Теренций Публий из Карфагена

Требования к возможностям языка

Возможность автоматизированного синтеза средств защиты и анализа защищенности компьютерной системы

↓

Использование формализма, позволяющего задавать и анализировать знания об угрозах, системе защиты и защищаемой системе, представленной в виде семантической сети

↓

Логический процессор
(модуль логического вывода)

↗ ↘

Функциональное описание атаки, функциональное описание системы защиты, вопрос о консистентности системы защиты.

Оценка уязвимости системы, набор потенциально успешных функциональных атак, наличие противоречий в системе защиты

Дескрипционные логики (ДЛ)

Семейство современных языков для формального описания знаний, обеспечивающих баланс между выразительной мощностью и вычислительной сложностью.

ДЛ тесно связаны с языками концептуального моделирования (например, ER-моделями и UML), что делает их подходящей базой для синтеза структуры модулей системы защиты.

Базовые понятия дескрипционных логик (ДЛ)

Концепт – одноместный предикат
Роль – двухместный предикат
Индивид – конкретная сущность

База знаний ДЛ состоит из двух компонентов:

1) Tbox – терминология (задает связь концептов и ролей)
2) Abox – набор фактов, т.е. утверждений об индивидах, сформулированных в терминах TBox

Комплексные концепты и роли формируются на основе атомарных с помощью конструкторов

Выразительная мощность конкретного языка, основанного на дескрипционных логиках, ограничена набором используемых конструкторов

Семантика дескрипционных логик (ДЛ)

Интерпретация I состоит из непустого множества ΔI (области интерпретации) и интерпретирующей функции, ставящей в соответствие каждому концепту A множество $A^I \subseteq \Delta^I$, а каждой роли R – бинарное отношение $R^I \subseteq \Delta^I \times \Delta^I$.

Семантика аксиом TBox: интерпретация I удовлетворяет аксиоме вхождения $C \sqsubseteq D$, если $C^I \subseteq D^I$, и она удовлетворяет эквивалентности $C \equiv D$, если $C^I \equiv D^I$. Если T является набором аксиом, тогда I удовлетворяет T, если I удовлетворяет каждому элементу T.

Семантика аксиом ABox:
$I = (\Delta^I, \cdot^I)$ отображает атомарные концепты и роли в множества и отношения, каждому имени индивида a ставит в соответствие элемент $a^I \in \Delta^I$. Интерпретация I удовлетворяет утверждению о понятии $\mathrm{C(a)}$, если $a^I \in C^I$, и удовлетворяет утверждению о роли $\mathrm{R(a, b)}$, если $(a^I, b^I) \in R^I$.

Анализ состояния безопасности системы по ее семантическому графу

- **Распространимость информации** - множество вершин, в которые может попасть информация из определенной вершины. Рассматривая существующие пути из вершины, обладающей «ценной» информацией, можно определить, насколько далеко и насколько быстро могут быть переданы защищаемые данные – как при нормальном функционировании системы, так и в случае нарушения политики безопасности.

- **Достижимость информации** - множество субъектов, имеющих доступ к определенной информации. Это обратная, по отношению к распространимости, характеристика, которая может служить основой, например, для вычисления вероятности компрометации каких-либо данных – описание каждого субъекта содержит ряд параметров, влияющих на эту вероятность (активность, уровень доступа и т.п.).

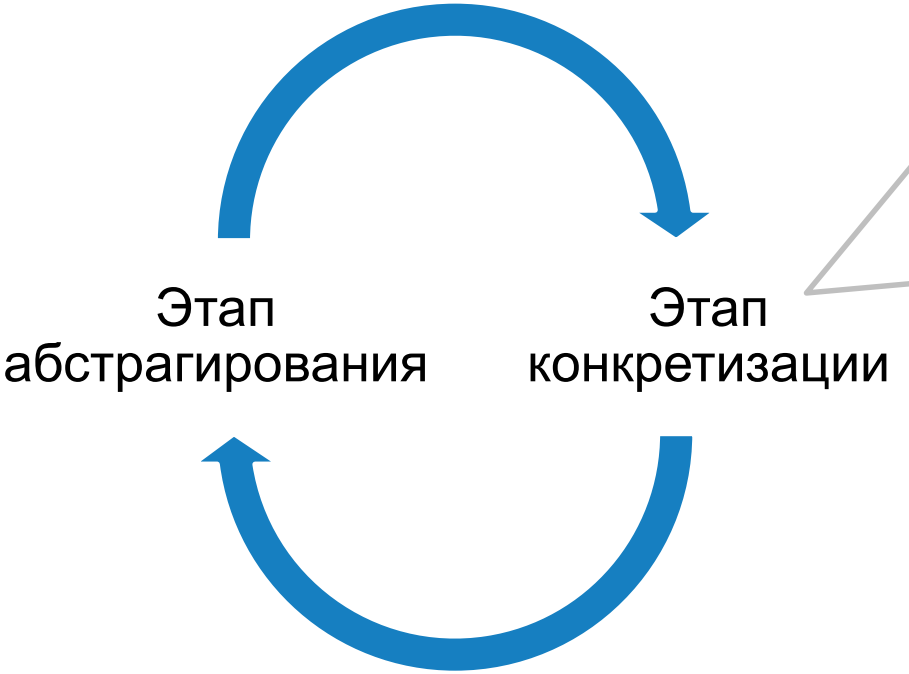
- **Информированность субъекта** - множество содержащих информацию вершин, доступных определенному субъекту. Этот параметр отражает неформальную «привилегированность» субъекта, что влияет, в том числе, на значимость его компрометации для нарушителя.

Раздел 4.
Сценарий проведения моделирования безопасности

Тысяча путей уводит от цели и лишь один ведет к ней.

Мишель Эйкем де Монтень

Основные этапы моделирования



Условия осуществления этапа конкретизации:

- ✓ наличие базы знаний, содержащей возможные конструктивные варианты реализации узла
- ✓ Составление матрицы маршрутов с учетом конкретных протоколов, параметров, ограничений и характеристик связи

Идеология универсального решения задачи безопасности – извлечение знаний о процессе за счет сохранения неопределенности описания при цикле уточнения модели.

Моделирование безопасности системы

<table>
<tr><td colspan="2">Описание структуры системы как минимум на двух уровнях: транспортном и логическом</td></tr>
<tr><td>Система задается набором элементов (каждый выполняет какую-либо функцию из заданного набора) и связей между ними</td><td rowspan="2">Над системой заданы два информационных потока:
1) рабочий (определяет информационное назначение системы);
2) управляющий (задает команды, инициирующие функции узлов)</td></tr>
<tr><td>Каждый узел задается термом (имя, функциональное назначение)</td></tr>
</table>

Моделирование процесса атаки

При формализации сценария атаки нужно четко определить:

1) Факт преодоления защиты:
   - ✓ нахождение маршрута, который не защищен – цепочки отношений R, на которой не реализованы адекватные функции защиты L_{ij};
   - ✓ превышение меры интенсивности воздействия над вероятностью защиты $p(Rul)$ (самый простой, но нежелательный вариант);
   - ✓ нахождение в защите бреши: применение неучтенной уязвимости, кража пароля – реализация функций из множества L^{new}, приводящих к нарушению ПБ, заданной Rul.

2) Факт достижения цели атаки:
   - ✓ внедрение нового объекта O_i;
   - ✓ уничтожение существующего узла O_i;
   - ✓ разрыв связей – изменение отношений $\{O_i\}$;
   - ✓ построение маршрута к критическому ресурсу (наличие потока F^R или F^W к критическому ресурсу)
   - ✓ достижение заданной вероятностной оценки преимущества защиты $p(Rul)$ или нападения.

Раздел 5.
Пример применения предлагаемого подхода

Средний путь самый безопасный

Публий Овидий Назон

Архитектура системы моделирования

Цель проведения эксперимента

1. Оценка защищенности сегмента Интернета вещей к атаке подмены данных от конечного устройства (GPS-датчика) на основе анализа дублирующих маршрутов, по которым могут передаваться потенциально подменяемые данные (в случае использования избыточных связей или функционирования конечного устройства в рамках нескольких информационных процессов, реализованных в сегменте Интернета вещей)

2. Выявление возможности утечки данных с критически важного информационного ресурса на основе анализа семантических свойств совокупности данных, потенциально доступных нарушителю на внешнем периметре сегмента Интернета вещей

Экспериментальные исследования: моделирование атаки на сегмент Интернета вещей

Виртуальные и физические устройства Интернета вещей, оснащенные GPS-датчиками и сенсорами освещенности (~1000 устройств)

Результаты экспериментального применения предлагаемого подхода

1. Выявление факта наличия уязвимости системы к заданному функциональному типу атаки (подмена данных от сенсоров Интернета вещей)
2. Генерация набора требований к системе защиты, обеспечивающей устойчивость системы по отношению к моделируемым атакам
3. Оценка вероятности доступа к критическому ресурсу Интернета вещей на основе анализа маршрутов семантической сети системы

Перспективные направления применения функциональных моделей безопасности

Контроль безопасности состояния системы в виде реализации информационного процесса и его параметров при соблюдении политики безопасности

Описание полного множества атак в виде искажения семантического графа системы, что дает возможность описания новых (неизвестных) атак

Автоматизация построения систем защиты с учетом заданного множества функциональных атак (а не их конкретных видов)

Моделирование информационного противоборства

Доказательство достижимости условий безопасности

Кафедра ИБКС
ФГАОУ ВО «СПбПУ»

Санкт-Петербург, ул.Политехническая, д.29,
Главное здание, К. 173

Тел: +7(812) 552-64-89,
552-76-32

Web: IBKS.FTK.SPBSTU.RU
E-mail: ZEG@ IBKS.FTK.SPBSTU.RU