

Теория информационной безопасности и методология защиты информации

Лекция 5

Модели разграничения доступа. Часть 1

к.т.н., доцент ФБИТ
Коржук Виктория Михайловна

весна, 2022

Предыдущая лекция



1. Надежная система ИБ
2. Итоговые события нарушения ИБ
3. Функции ЗИ
4. Множество задач защиты
5. Классы задач ЗИ

Модель

безопасности

1. выбор и обоснование архитектуры ИС;
 2. подтверждение свойств защищенности разрабатываемых систем;
 3. составление формальной спецификации модели безопасности.
1. Заказчик (потребитель)
 2. Разработчик (производитель)
 3. Эксперт (аудитор)

Quiz

Методы обеспечения защищенности информации

К обеспечению конфиденциальности относятся...

- ограничение и разграничение доступа
- информационное скрывтие
- введение информационной избыточности
- методы надежного хранения, преобразования и передачи информации
- нормативно-административное побуждение и принуждение

К обеспечению целостности относятся...

- ограничение и разграничение доступа
- информационное скрывтие
- введение информационной избыточности
- методы надежного хранения, преобразования и передачи информации
- нормативно-административное побуждение и принуждение

К обеспечению доступности относятся...

- ограничение и разграничение доступа
- информационное скрывтие
- введение информационной избыточности
- методы надежного хранения, преобразования и передачи информации
- нормативно-административное побуждение и принуждение

Дискретное время

Подмножество субъектов
доступа S

Подмножество объектов
доступа O

Объект доступа - пассивная
сущность,

может быть источником
порождения новых субъектов.

Субъект - активная сущность,

может порождать новые
объекты

и влиять на порождение новых
субъектов.

Пользователь - лицо или внешний фактор,

идентифицированный,
аутентифицированный и авторизованный,

управляющий субъектом/ами

воспринимающий объекты

получающий информацию о ИС.



Чем, все же, отличается пользователь от субъекта?

Collaborate!

Чем, все же, отличается пользователь от субъекта?

Порождение и ассоциация

Порождение

O_i называется ИСТОЧНИКОМ для S_m ,
если существует S_j ,
который воздействовал на O_i ,
и получился S_m .

Create (S_j , O_i) $\rightarrow S_m$

S_j - активизирующий для S_m .

Ассоциация

O_i в момент времени T_k ассоциирован с
субъектом S_m , если

состояние O_i повлияло на состояние S_m
в следующий момент времени.



Приведите примеры порождения в ИС

Collaborate!

Приведите примеры порождения в ИС



Приведите примеры ассоциации в ИС

Collaborate!

Приведите примеры ассоциации в ИС

Потоки

Поток информации между O_i и O_j -
действие S_n
над объектом O_j
зависящее от O_i .

Stream $(S_n, O_i) \rightarrow O_j$

Поток=права

информации

Функционально-
ассоциированные объекты

vs

Ассоциированный объекты-
данные

Объясните на при  в чем разница...

... между функционально-ассоциированными объектами и ассоциированными объектами-данными

Collaborate!

Объясните на примере, в чем разница...

Доступ и правила разграничения

Доступ S_m к O_j -
порождение S_m потока
между O_j и O_i .

Существует множество потоков P , состоит из
непересекающихся множеств P_L
(безопасные) и P_N (нарушающие ИБ).

Правила разграничения доступа -
формально описанные потоки,
принадлежащие множеству P_L .



Poll

Что вы чувствуете по отношению к поражению, ассоциации, потокам и безопасным потокам?

- ☐ Я все понял(а)!
- ☐ Ну, в целом понятно.
- ☐ Какая-то теоретическо-методическая ерунда, но жить можно.
- ☐ Можно я пойду?
- ☐ Я не понимаю ничего.

Монитор безопасности.

АКСИОМЫ.


Аксиома 1. В защищенной ИС в любой момент времени любой S и O должны быть идентифицированы и аутентифицированы.



Монитор безопасности (МБ) - субъект осуществления принятой политики безопасности.

Аксиома 2. В защищенной ИС должна присутствовать активная компонента с соответствующим объектом(ами)-источниками, которая осуществляет управление доступом и контроль доступа Ss к Oo.

Требования к МБ:

1. Полнота
2. Изолированность
3. Верифицируемость
4. Непрерывность



Непрерывность	отслеживания и та.	проверяться и тестироваться.
Верифицируемость	 	МБ должен функционировать

Matching Pairs

МБ. АКСИОМЫ

Аксиома 3. Для реализации принятой политики ИБ необходима (должна существовать) информация и Оо, ее содержащие.

Следствие 3.1. В ИС существуют S_s , которые не инициализируют и не управляются пользователями (системные процессы).

Следствие 3.2. Ассоциированный с МБ S , содержащий И о системе разграничения доступа - наиболее важный с для ИБ.

Следствие 3.3. В защищенной системе может существовать доверенный пользователь (админ), S_s которого имеют доступ к ассоциированному с МБ объекту-данным для управления системой разграничения доступа.



7 7 Дискреционная модель разграничения доступа

51 views • Dec 15, 2019

2 0 SHARE SAVE ...

alexander lee

SUBSCRIBE

You're signed out of YouTube
Sign in to like videos, comment, and subscribe.
GOT IT



7 9 Роль в разграничении доступа
alexander lee
31 views • 4 months ago



5. Типы моделей
CARECECO
Recommended for you



1 WE~1
alexander lee
Recommended for you
New



Централизованное управление...

<https://www.youtube.com/watch?v=ya8Qdo9aeHo>



Лекция 11
Загрузка...
alexander lee
2 views • 3 days ago
New

Опишите достоинства и недостатки
дискреционной модели



Collaborate!

Опишите достоинства и недостатки дискреционной модели

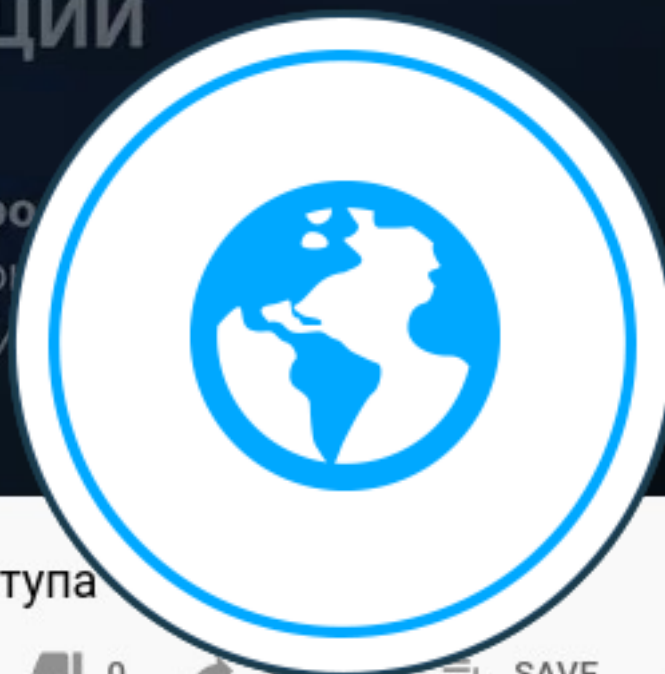


ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

КУРС ЛЕКЦИЙ

ЗАЩИТА ИНФОРМАЦИИ

Сорокин Александр Владимиро
Старший преподаватель кафедры
компьютерной безопасности МИ



7 8 Мандатная модель разграничения доступа

68 views • Dec 15, 2019



2



0



SHARE



SAVE



alexander lee

SUBSCRIBE

You're signed out of YouTube

Sign in to like videos, comment, and subscribe.

GOT IT

4:40 4 months ago



Лекция 7 Веб
формы в Django...

alexander lee
Recommended for
you

New



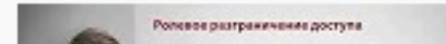
Sounds of nature,
birds singing,...

TopRelaxMusic
Recommended for
you



Централизованн
управление...

Код Безопаснос...
381 views •
2 years ago



7 9 Ролевая

<https://www.youtube.com/watch?v=sIPpC2cgWUc>

5:27 4 months ago



6 1
Невырожденн...

alexander lee
Recommended for
you

New

Опишите достоинства и недостатки мандатной модели



Collaborate!

Опишите достоинства и недостатки мандатной модели



7 9 Ролевая модель разграничения доступа

34 views • Dec 15, 2019

1 0 SHARE SAVE ...

alexander lee

SUBSCRIBE

You're signed out of YouTube

Sign in to like videos, comment, and subscribe.

GOT IT

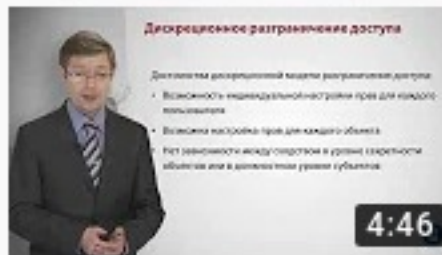
4:30 4 months ago



Лекция 4
Синтаксис...
alexander lee
Recommended for you
New



RBAC & ABAC:
гибридное...
CUSTIS
Recommended for you

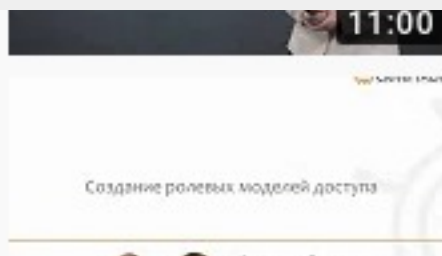


7 7
Дискреционная...
alexander lee
45 views •
4 months ago



1 WE~1

<https://www.youtube.com/watch?v=MU5ZFazWYQo>



11:00 New
Создание ролевых...
Cleverics (official)
1K views •
4 years ago

Опишите достоинства и недостатки ролевой модели



Collaborate!

Опишите достоинства и недостатки ролевой модели

Гарантирование выполнения политики безопасности

Компьютерная система безопасна тогда и только тогда, когда Ss не имеют возможности нарушить или обойти установленную в ИС политику безопасности.

Наличие МБ - необходимое условие безопасности.

Безопасность МБ - условие достаточности.

Правила разграничения доступа должны включать в себя правила порождения Ss пользователями.

Монитор безопасности объектов (МБО) - субъект, действующий при возникновении потока между любыми Oo , порождаемого любыми Ss , разрешающий только потоки из PL .

Монитор безопасности субъектов (МБС) - субъект, действующий при любом порождении Ss , разрешающий порождение Ss из установленного подмножества пар активизирующих Ss и объектов-источников.

Тождественность

O_i и O_j тождественны в момент времени t , если они совпадают как слова, записанные на одном языке.

$$O_i[t] = O_j[t]$$

S_i и S_j тождественны в момент времени t , если попарно тождественны все ассоциированные с ними O_o .

Порожденные S_s тождественны, если тождественны все порождающие S_s и O_o -источники.

S_i и S_j называются невлиющими друг на друга (КОРРЕКТНЫМИ),

если в любой момент времени отсутствует поток между любыми O_{ik} и O_{jl} , ассоциированными соответственно с O_i и O_j .

S_i и S_j называются абсолютно невлиющими друг на друга (АБСОЛЮТНО КОРРЕКТНЫМИ),

если их множества ассоциированных O_o не имеют пересечения.

Приведи примеры...



1) тождественных объектов; 2) 2 абсолютно корректных субъектов.

Collaborate!

Приведите примеры...

Достаточные условия гарантий безопасности

1. МБО разрешает порождение потоков только из множества PL , если все существующие в системе Ss абсолютно корректны относительно его и друг друга.

2. Если в абсолютно изолированной ИС существует МБО и порождаемые Ss абсолютно корректны относительно МБО, а также существует МБС, которые абсолютно корректны относительно МБО, то в ИС реализуется только доступ, заданный политикой/моделью разграничения доступа.

ИС называется замкнутой по порождению Ss , если в ней действует МБС, разрешающий порождение только фиксированного конечного подмножества Ss для любых Oo -источников.

Множество Ss ИС называется изолированным, если в ней действует МБС и Ss из порождаемого множества корректны относительно друг друга и МБС.

Базовая теорема

ИПС

Операция порождения субъектов называется порождением с контролем неизменности O , если для любого момента времени $t > t_0$, порождение возможно только при тождественности O -источника относительно t_0 .

$$O_m[t] = O_m[t_0]$$

$$S_i[t_1] = S_i[t_2], \text{ если } t_1 = t_2$$

Если в изолированной ИС, в которой действует порождение S_s с контролем неизменности O , в момент времени t_0 через любой S к любому O существуют только потоки, не противоречащие условию корректности (абсолютной корректности), то в любой момент времени $t_k > t_0$ ИС также остается изолированной (абсолютно изолированной).

Poll

Как оно?

- ☐ Я жив(а)!
- ☐ Пойду еще раз все прочитаю...
- ☐ Я так ничего и не понял(а)...
- ☐ Скорее бы лето. Хотя нет, там же экзамен будет по этой беде...
- ☐ Хочу CTF!