Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

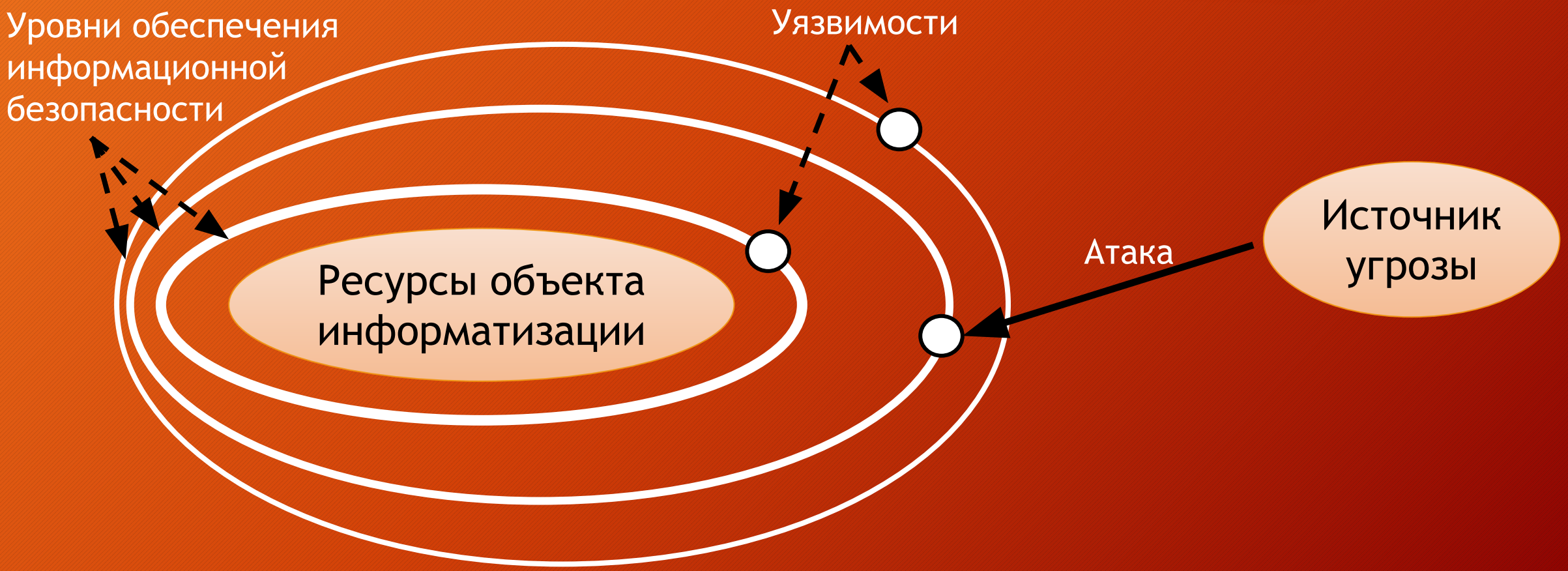
Модель нарушителя
Классификация уязвимостей безопасности
Основные типы атак на информационные ресурсы

Выполнил студент группы ИБ2-1
Однорал Александр

Руководитель:

доц. Кружилов С.И.

Взаимосвязь понятий



Классификация уязвимостей и атак

Цель исследования

1. Создание имитационной модели работы веб-приложения → Обработка результатов моделирования

2. Получить ответ на вопрос:
на что эффективнее затрачивать средства →
- Улучшение технических характеристик объекта
- Обеспечение информационной безопасности объекта

Описание объекта исследования

Описание модели

Характеристики веб-приложения при условиях работы в «час пик»:

1. Период моделирования (2 часа)
2. Количество пользовательских запросов (6000 запросов)
3. Вероятность того, что пользователь является злоумышленником (0,4%)
4. Время отправки запросов (случайная величина с нормальным законом распределения с математическим ожиданием 60 минут и среднеквадратическим отклонением 10 минут)

Описание модели

Изменяемые параметры модели:

Затрата средств на улучшение характеристик объекта

Затрата средств на улучшение степени защищенности объекта

1. Время обработки запросов

СВ с нормальным законом распределения с математическим ожиданием 0,7 ▫ 0,4 секунды и среднеквадратическим отклонением 0,2 ▫ 0,1 секунды

СВ с нормальным законом распределения с математическим ожиданием 0,7 секунды и среднеквадратическим отклонением 0,2 секунды

2. Время вывода «из строя»

СВ с нормальным законом распределения с математическим ожиданием 6 минут и среднеквадратическим отклонением 1 минута

СВ с нормальным законом распределения с математическим ожиданием 6 ▫ 3 минуты и среднеквадратическим отклонением 1 минута

Описание модели

Изменяемые параметры модели:

Затрата средств на улучшение характеристик объекта

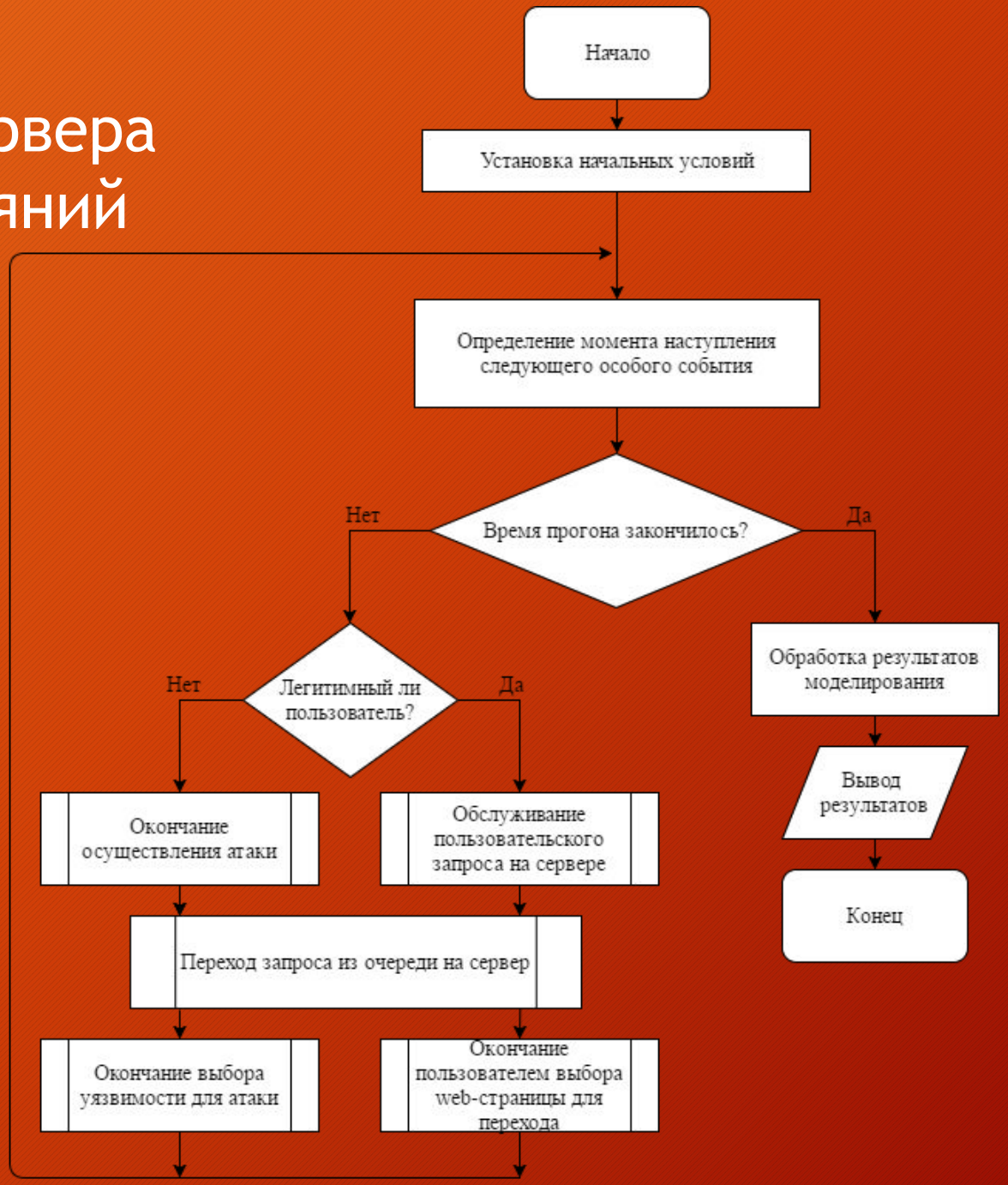
Затрата средств на улучшение степени защищенности объекта

3. Степень защищенности уязвимостей

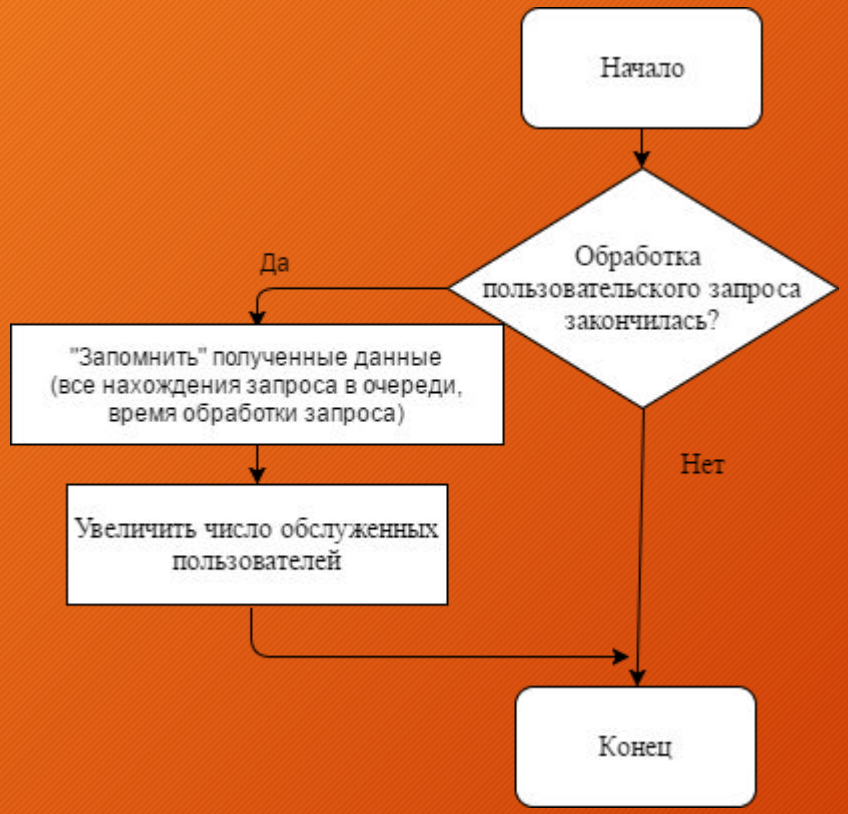
```
'attack_type': 'man-in-the-middle',
'vulnerability': 'sensitive data exposure',
'degree of protection': 0.75

'attack_type': 'using components with known vulnerabilities',
'vulnerability': 'third-party components vulnerabilities',
'degree of protection': 0.64

'attack_type': 'SQL injection',
'vulnerability': 'invalid input validation',
'degree of protection': 0.82

'attack_type': 'cross site scripting',
'vulnerability': 'invalid input validation',
'degree of protection': 0.73

'attack_type': 'DDoS',
'vulnerability': 'server configuration',
'degree of protection': 0.78
```

```
'attack_type': 'man-in-the-middle',
'vulnerability': 'sensitive data exposure',
'degree of protection': 0.85

'attack_type': 'using components with known vulnerabilities',
'vulnerability': 'third-party components vulnerabilities',
'degree of protection': 0.74

'attack_type': 'SQL injection',
'vulnerability': 'invalid input validation',
'degree of protection': 0.92

'attack_type': 'cross site scripting',
'vulnerability': 'invalid input validation',
'degree of protection': 0.83

'attack_type': 'DDoS',
'vulnerability': 'server configuration',
'degree of protection': 0.88
```

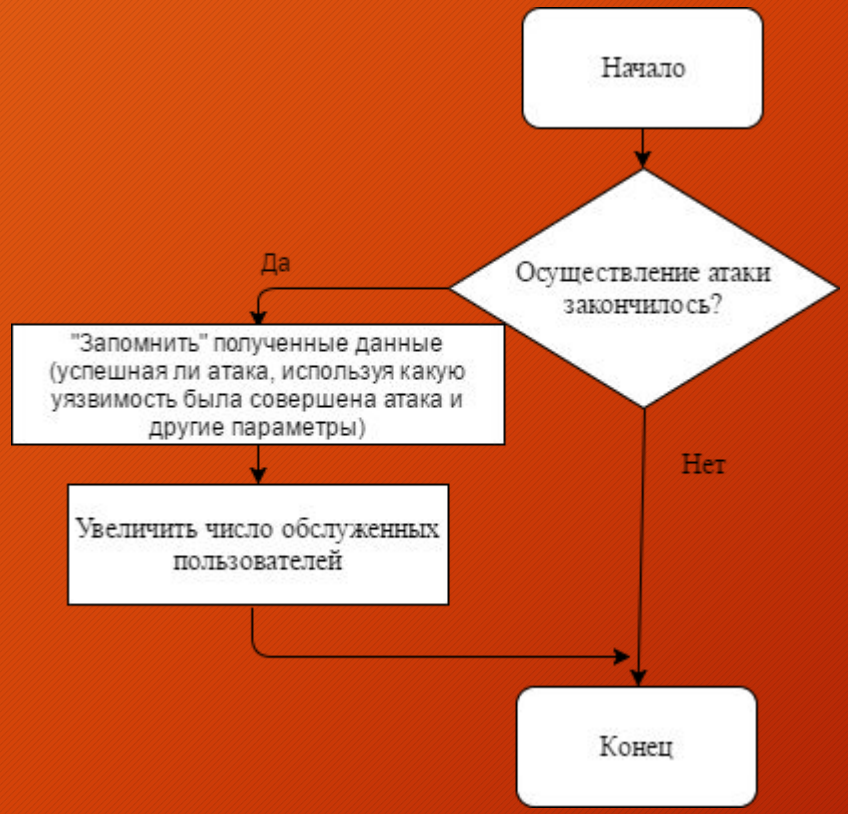
Блок-схема алгоритма моделирования работы сервера по принципу особых состояний



«Обслуживание запроса на сервере»



«Окончание осуществления атаки»



«Переход запроса из очереди на сервер для дальнейшей обработки»

«Окончание пользователем выбора веб-страницы для перехода»

«Окончание выбора уязвимости для атаки»

Результат моделирования

Параметры модели	Моделирование при условии затрат средств на улучшение производительности модели	Моделирование при условии затрат средств на повышение информационной безопасности модели
Общее количество запросов	6000	6000
Количество обработанных сервером запросов	5550	5923
Количество необработанных запросов	450	77
Время обработки запросов сервером (чч:мм:сс)	0:36:56	1:08:20
Количество пользователей - злоумышленников	21	26
Количество успешных атак на известные уязвимости модели	8	4
Время нахождения сервера в «нерабочем» состоянии (чч:мм:сс)	0:49:07	0:11:08

Список использованных источников

- Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: Лето, 2011. — С. 8-13.
- Международный стандарт информационной безопасности ISO/IEC 27005:2008.
- [Электронный ресурс] https://www.owasp.org/index.php/Category:Attack (дата обращения - 22.05.2017)
- Коробейников А.Г., Трояков И.Б., Жаринов И.О., Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий: монография / Под ред. П.П. Парамонова. СПб: Изд-во ООО «Студия «НП-Принт», 2012. – 115 с.
- Советов Б.Я. Моделирование систем: учебник для ВУЗов / Б.Я. Советов, С.А. Яковлев, – М.: Высшая школа, 2005. – 343с.
- Андреев В.В. Моделирование систем: уч. Пособие / В.В. Андреев, – Чебоксары: Изд-во Чуваш. ун-та, 2004. – 304с.
- [Электронный ресурс] http://bdu.fstec.ru/threat (дата обращения – 19.05.2017)
- [Электронный ресурс] http://bdu.fstec.ru/vul (дата обращения – 19.05.2017)
- Девянин П.Н. Теоретические основы компьютерной безопасности: Учебное пособие для вузов - М.: Радио и связь, 2000. П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков.

Спасибо за внимание