# Дерево угроз и модель нарушителя для удостоверяющего центра

Подгорная Анна и Хапова Полина

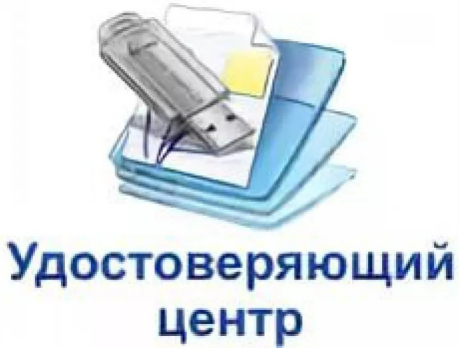
Цель:

Практическое освоение базовых навыков работы в Удостоверяющем центре.

Задачи:

- изучение нормативной документации в области ЭП и регламентов работы УЦ;
- выполнение типовых задач УЦ;
- построение дерева угроз;
- построение модели нарушителя.

# Удостоверяющий центр




Доверенная организация, которая имеет право выпускать сертификаты электронной подписи юридическим и физическим лицам.

# Основные определения

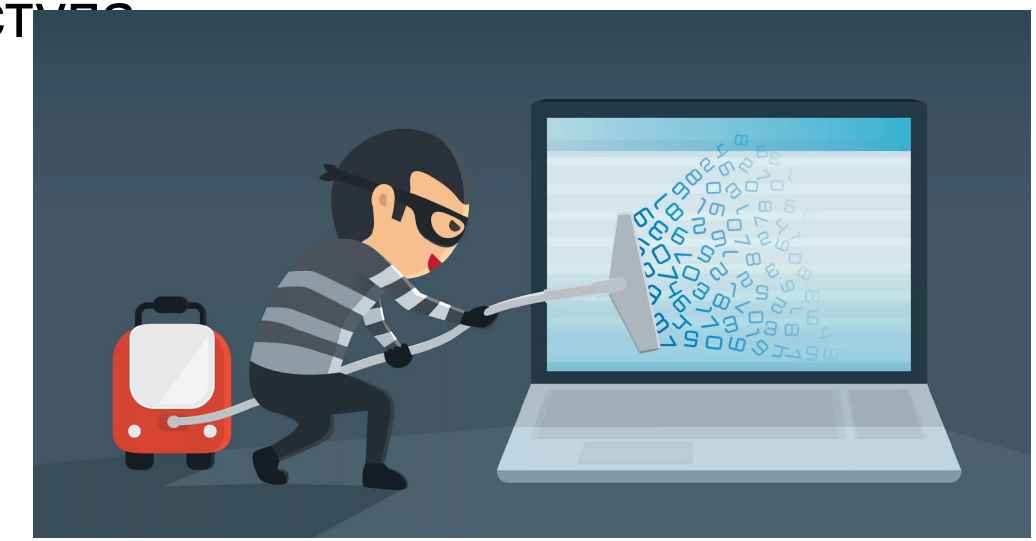
Угроза - возможность преднамеренного или случайного действия, которое может привести к нарушениям безопасности хранимой или обрабатываемой информации и программ.

Дерево угроз - иерархический способ представления угроз.

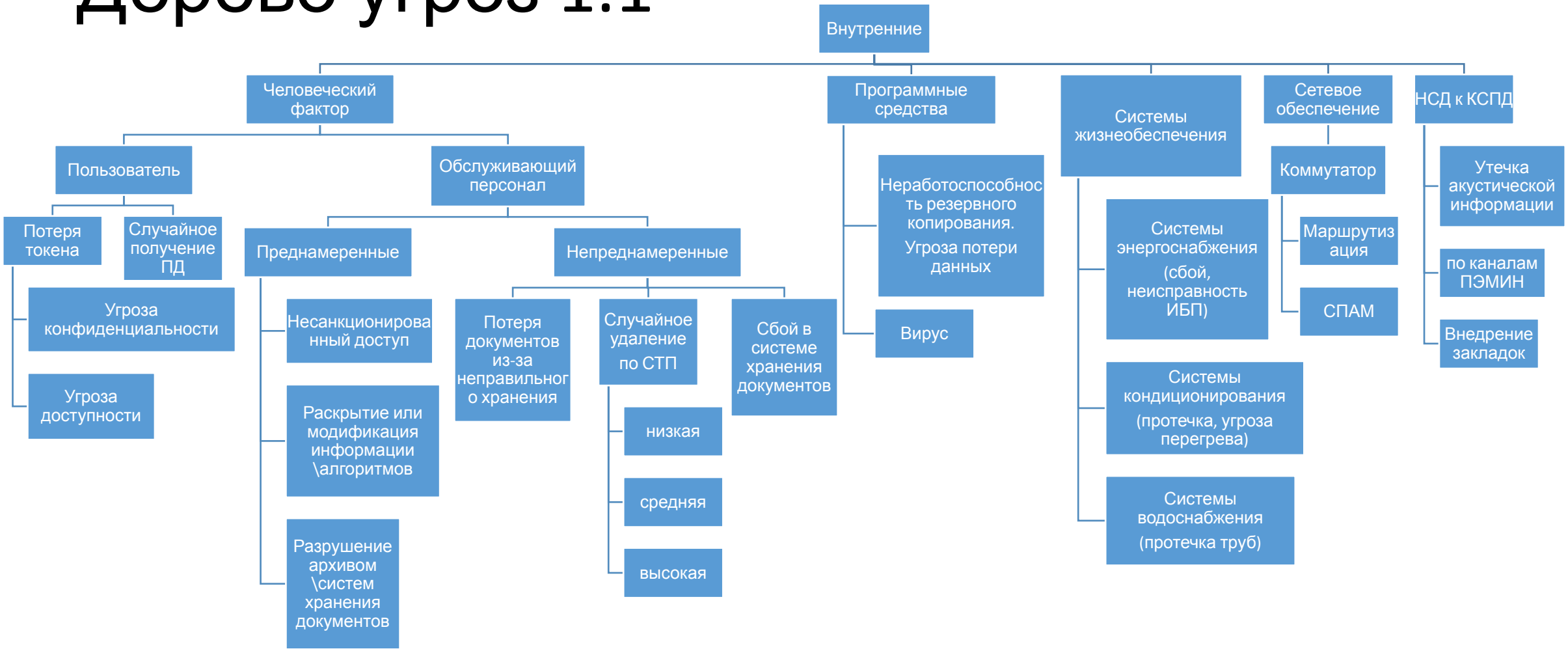
# Основные определения

Нарушитель ИБ — это лицо, которое предприняло попытку выполнения запрещенных операций по ошибке, незнанию или осознанно со злым умыслом и использующее для этого различные возможности, методы и средства.

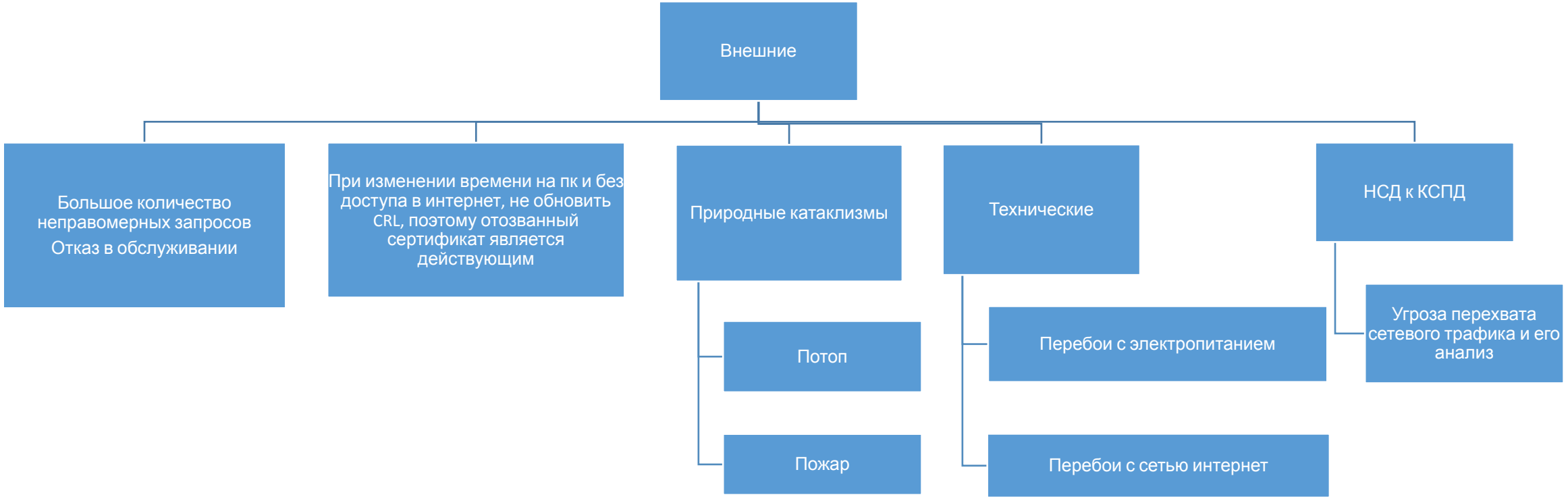
Модель нарушителя - абстрактное (формализованное\неформализованное) описание нарушителя правил разграничения доступа



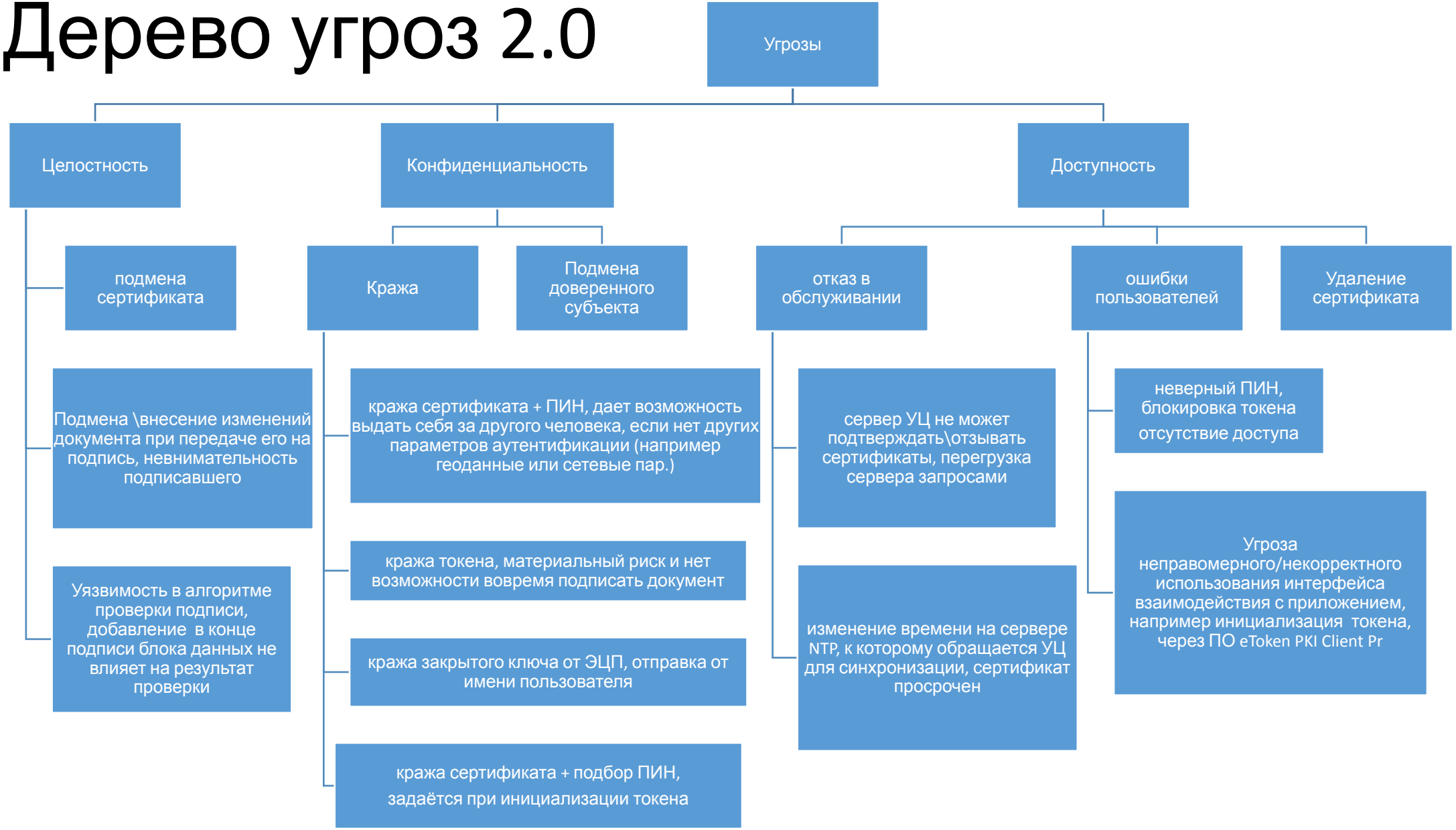
# Дерево угроз 1.1



# Дерево угроз 1.2



# Дерево угроз 2.0



# Модель нарушителя

| Наименование | Тип нарушителя | Уничтожение данных | Внесение изменений в ПО | Продажа конфид. данных | Раскрытие алгоритмов УЦ | Вывод из эксплуатации оборудования | Внесение изменений в данные |
|---|---|---|---|---|---|---|---|
| **Дирекция** | Внутренний | Высокая | Низкая | Средняя | Высокая | Средняя | Высокая |
| **Администратор УЦ** | Внутренний | Высокая | Низкая | Средняя | Высокая | Средняя | Высокая |
| **Оператор УЦ** | Внутренний | Высокая | Низкая | Средняя | Средняя | Средняя | Высокая |
| **Программист, ТО** | Внутренний | Высокая | Высокая | Средняя | Высокая | Высокая | Высокая |
| **Администратор безопасности** | Внутренний | Средняя | Средняя | Средняя | Высокая | Средняя | Средняя |
| **Практикант** | Внутренний/ Внешний | Высокая | Низкая | Высокая | Низкая | Средняя | Низкая |
| **Временный сотрудник** | Внутренний | Высокая | Низкая | Высокая | Средняя | Средняя | Средняя |
| **Уборщица** | Внутренний | Средняя | Низкая | Низкая | Низкая | Высокая | Низкая |
| **Клиент** | Внешний | Средняя | Низкая | Низкая | Низкая | Средняя | Низкая |

# Модель нарушителя

| № | Вид нарушителя | Тип по ФСТЭК | Группа | Тип по ФСБ | Возможные угрозы |
|---|---|---|---|---|---|
| 1 | Клиенты | Внешний | - | Н1 | Физическое уничтожение данных или оборудование |
| 2 | Конкурирующие организации | Внешний | - | Н4 | Несанкционированное получение и раскрытие конфиденциальной информации |
| 3 | Практиканты | Внешний | - | Н1 | Непреднамеренные, неосторожные или неквалифицированные действия<br>Физическое уничтожение данных или оборудование. Раскрытие полученной информации |
| 4 | Дирекция | Внутренний | Группа 5 | Н3 | Уничтожение\модификация данных, раскрытие конфиденциальной информации УЦ |
| 5 | Администратор УЦ | Внутренний | Группа 5 | Н3 | Уничтожение\модификация данных<br>Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |
| 6 | Оператор УЦ | Внутренний | Группа 5 | Н3 | Уничтожение\модификация данных |
| 7 | Программист ,ТО | Внутренний | Группа 7,8 | Н4 | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки.<br>Непреднамеренные, неосторожные или неквалифицированные действия |
| 8 | Администратор безопасности | Внутренний | Группа 6 | Н3 | Раскрытие конфиденциальной информации УЦ<br>Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |
| 9 | Временный сотрудник | Внутренний | Группа 2 | Н3 | Неосторожные или неквалифицированные действия<br>Продажа конфиденциальной информации с целью получения материальной выгоды |
| 10 | Уборщица | Внутренний | Группа 1 | Н2 | Ущерб оборудованию |

# Заключение

- приобретены навыки работы с нормативной документацией;
- изучена нормативная документация в области ЭП и регламенты работы УЦ;
- построены и проанализированы деревья угроз, модель нарушителя.

Спасибо за внимание!!!