

## 1. Классификация угроз:

- По аспекту информационной безопасности (доступность, целостность, конфиденциальность):
  - a. Dos атака
- По компонентам информационной системы (Данные, программы, аппаратура)
- По способу осуществления (случайные, преднамеренные, техногенного характера)
- По расположению источника угроз (Внутри, вне)

## 2. Исследовать БДУ ФСТЭК:

### Доступности:

УБИ.014: Угроза длительного удержания вычислительных ресурсов пользователя

Описание: Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загружённом состоянии путём осуществления им многократного выполнения опред. Деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачи.

УБИ.014: Угроза длительного удержания вычислительных ресурсов пользователями		Вид ▾
Описание угрозы	Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определенных деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя	
Источники угрозы	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	
Объект воздействия	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	
Последствия реализации угрозы	Нарушение доступности	

## Конфиденциальности:

УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути

Описание: Угроза заключается в возможности получения нарушителем доступа к скрытым каталогам или файлам посредством различных воздействий на файловую систему.

УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути		Вид ▾
Описание угрозы	Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях: наличие у нарушителя прав доступа к некоторым объектам файловой системы; отсутствие проверки вводимых пользователем данных; наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью	
Источники угрозы	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	
Объект воздействия	Объекты файловой системы	
Последствия реализации угрозы	Нарушение конфиденциальности	

## Целостности:

УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации

Описание: Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или другие периферийные устройства.

УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации		Вид ▾
Описание угрозы	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок	
Источники угрозы	Внешний нарушитель с высоким потенциалом Внутренний нарушитель с низким потенциалом	
Объект воздействия	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение	
Последствия реализации угрозы	Нарушение целостности	