**Отчёт**

Категория: аппаратное ПО  
**Объекты воздействия:**

Аппаратное обеспечение

Cистемное программное обеспечение

**Нарушители:**

Специальные службы иностранных государств : Внутренний

Террористические экстремистские группировки : Внешний

Преступные группы (криминальные структуры) : Внешний

Отдельные физические лица (хакеры) : Внешний

Конкурирующие организации : Внешний

Разработчики программных программно аппаратных средств : Внешний

Лица обеспечивающие поставку программного обеспечения : Внешний

Поставщики услуг связи, вычислительных услуг : Внешний

Лица привлекаемые для установочных, пускналадочных работ : Внешний

Лица обеспечивающие функционирование систем и сетей или обеспечевающих систем оператора : Внешний

Авторизованные пользователи систем и сетей : Внешний

Системные администраторы и администраторы безопасности : Внешний

Бывшие (уволенные) работники (пользователи) : Внешний

# Класс защищённости (сделать возможность для нескольких):

**К3**

# Вид риска/Негативные последствия: на основе ввода пользователя:

Ущерб физическому лицу

Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью

# Способы реализации:

# Техники тактики и угрозы:

**Угрозы:**  
  
  
Угроза избыточного выделения оперативной памяти Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей.   
Данная угроза обусловлена наличием слабостей механизма контроля выделения оперативной памяти различным программам.   
Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии

Соответствующие техники тактики:

Угроза неправомерного ознакомления с защищаемой информацией Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей.   
Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств.   
Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.

Соответствующие техники тактики:

Угроза несанкционированного использования привилегированных функций BIOS Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI.   
Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала

Соответствующие техники тактики: