**УБИ.126: Угроза подмены беспроводного клиента или точки доступа**

*В чем заключается угроза?*

Угроза заключается в возможности получения нарушителем аутентификационной или другой защищаемой информации, передаваемой в ходе автоматического подключения точек беспроводного доступа или клиентского программного обеспечения к доверенным субъектам сетевого взаимодействия, подменённым нарушителем.

*Кто может реализовать угрозу?*

Внешний нарушитель с низким потенциалом. В данном случае такими нарушителями могут являться физические лица (хакеры), лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем, бывшие работники (пользователи).

*Как возможна её реализация?*

Реализация данной угрозы возможна в случае размещения нарушителем клиента или точки беспроводного доступа со специально сформированными параметрами работы (такими как MAC-адрес, название, используемый стандарт передачи данных и т.п.) в зоне доступности для дискредитируемых устройств беспроводного доступа.

*Каков объект воздействия?*

Объектами взаимодействия в данном случае являются точка беспроводного доступа, сетевое оборудование и программное обеспечение, АРМ пользователей и администратора.

*Каковы цели реализации угрозы?*

Целями реализации угрозы могут быть кража коммерческой тайны и её дальнейшая продажа недобросовестному конкуренту. В меньшей степени – передача информации о юридическом лице третьим лицам.

*Каковы последствия реализации угрозы?*

В результате реализации угрозы происходит нарушение конфиденциальности и доступности информации.

*Каковы меры защиты от данной угрозы?*

1. **Определение подозрительных клиентов или точек доступа.** При обнаружении клиентов или точек доступа, о создании которых системным администратором не было сообщено, пользователь должен соответственно обратиться к администратору для проведения проверочных мероприятий и ликвидации подозрительных клиентов/точек доступа.
2. **Проведение радиоэлектронной разведки местности.** При физической установке точки доступа в самой системе проведение радиоэлектронной разведки позволяет определить источник подозрительного ЭМИ и ликвидировать его.
3. **Использование межсетевого экрана и средств аудита событий.** С помощью данного программного обеспечения можно обнаружить и предотвратить вторжение злоумышленника, находящегося вне самой системы.
4. **Повышение квалификации пользователей системы.** При работе с системой пользователь должен осуществлять подключение только к проверенным точкам доступа/клиентам, находящимся непосредственно внутри самой системы. При обнаружении подозрительных объектов должен незамедлительно сообщим об этом системному администратору для проведения ряда соответствующих мероприятий.
5. **Систематическое обновление программного обеспечения.** Установка последних версий ПО позволяет ликвидировать уязвимости, что уменьшает число способов проникновения хакеров в систему.