Hlavním cílem této bakalářské práce je popis útoku na Niederreiterův kryptosystém vytvořený nad GRS kódy. Tento útok byl zveřejněn v roce 1992 Sidelnikovem a Šestakovem. Na začátku práce je uvedena problematika působení grupy na množině, která je použita v samotném útoku. Následuje stručný úvod do teorie samoopravných kódů, jsou popsány GRS kódy a představeny McEliecův a Niederreiterův kryptosystém, oba jako zástupci post-kvantové kryptografie. Další část práce je věnována samotnému útoku. Je ukázáno, jakým způsobem využijeme působení grupy na množině, dále je podrobně popsán průběh útoku a zmíněna jeho časová složitost. Vše je také ilustrováno na příkladech.