

**Взаимодействие МИД РФ с правоохранительными органами по противодействию угрозам в сфере информационной безопасности**

**Научный руководитель – Злоченко Яков Михайлович**

**Малыгина Анастасия Александровна**

*Студент (бакалавр)*

Уральский федеральный университет имени первого Президента России Б.Н.Ельцина,  
Институт государственного управления и предпринимательства, Екатеринбург, Россия

*E-mail: anastasia.m.2012@yandex.ru*

Статья посвящена анализу имеющихся угроз в сфере информационной безопасности и предотвращению их воздействия на информацию при взаимодействии МИД РФ с правоохранительными органами РФ. Актуальность данной темы увеличивается по мере развития интернет-технологий. Информационная безопасность - обеспечение конфиденциальности, целостности и доступности информации. Исходя из данного определения уже можно выделить основные угрозы информационной безопасности:

1. Угрозы конфиденциальности - несанкционированный доступ к данным.
2. Угрозы целостности - несанкционированная модификация, дополнение или уничтожение данных.
3. Угрозы доступности - ограничение или блокирование доступа к данным. [1]

Основными путями реализации угроз информации и безопасности информации являются:

- агентурные источники в органах управления и защиты информации;
- вербовка должностных лиц органов управления, организаций, предприятий и т. д.;
- перехват и несанкционированный доступ к информации с использованием технических средств разведки;
- использование преднамеренного программно-математического воздействия;
- подслушивание конфиденциальных переговоров в служебных помещениях, транспорте и других местах их ведения. [2]

Для того, чтобы этого не происходило существуют методы обеспечения безопасности информации такие как: препятствие, управление доступом, криптография, противодействие атакам вредоносных программ, регламентация, принуждение, побуждение. Так же МИД РФ плотно взаимодействует с такими структурами как ФСБ, МВД. Создано положение от 17 ноября 2008 года N 8722/996/562/350 о порядке информационного взаимодействия данных структур с целью выявления наличия обстоятельств, которые могут повлечь временное ограничение права гражданина Российской Федерации на выезд из Российской Федерации и отказ в выдаче паспорта, дипломатического паспорта и служебного паспорта, являющихся основными документами, удостоверяющими личность гражданина Российской Федерации за пределами территории Российской Федерации. Благодаря этому положению можно избежать утечки конфиденциальной информации путем ограничения выезда лиц, владеющих государственной тайной.

Существует еще один немаловажный документ-доктрина информационной безопасности, но на мой взгляд, в ней указаны не все направления обеспечения безопасности.

Поиск по сайту МИДа РФ [www.mid.ru](http://www.mid.ru) по словосочетанию «информационные угрозы» дал в общей сложности 1 500 документов, в основном датируемых 2015-2018 годами. Наибольшее количество упоминаний с данным словосочетанием связано с информационной

войной и кибератаками. Сейчас эффективность наступательных средств информационной войны, информационного оружия превосходит эффективность систем защиты информации. Главной целью нынешней информационной войны стран Запада против России является- ослабление России и дискредитация ее репутации за рубежом. [3]

На мой взгляд информационная безопасность России недостаточно развита, нужно увеличивать взаимодействие МИД с другими правоохранительными органами и совершенствовать систему обеспечения информационной безопасности.

### **Источники и литература**

- 1) Артемов А.В. Информационная безопасность. Курс лекций. Орел, 2014.
- 2) Гиляутдинов.ру: <http://www.galyautdinov.ru>
- 3) Мид.ру: <http://www.mid.ru>