# Диссер\_Информационная безопастность на промышленных предприятиях

Стр-82

[Введение](#_Toc462004907)

[I. Аналитическая часть](#_Toc462004908)

[1.1. Технико-экономическая характеристика предметной области и предприятия на примере АО «УСТЬ-КАМЕНОГОРСКИЙ ТИТАНО-МАГНИЕВЫЙ КОМБИНАТ»](#_Toc462004909)

[1.2. Анализ рисков информационной безопасности](#_Toc462004910)

[1.3. Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации на предприятии](#_Toc462004911)

[1.4. Выбор защитных мер](#_Toc462004912)

[II Проектная часть](#_Toc462004913)

[2.1 Комплекс организационных мер обеспечения информационной безопасности и защиты информации предприятия](#_Toc462004914)

[2.2 Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности и защиты информации и мониторинга безопасности предприятия](#_Toc462004915)

[III Выбор и обоснование методики расчёта экономической эффективности](#_Toc462004916)

[3.1 Выбор и обоснование методики расчёта экономической эффективности](#_Toc462004917)

[3.2 Расчёт показателей экономической эффективности проекта](#_Toc462004918)

[Заключение](#_Toc462004919)

[Список использованной литературы](#_Toc462004920)

# Заключение

В результате теоретического анализа установлено, что организационно-экономический механизм системы информационной безопасности представляет собой самоорганизующуюся систему заинтересованных лиц корпорации, форм и методов управления, рычагов и инструментов, правовых норм и организационно-экономических форм их использования в целях обеспечения надежной защищенности жизненно важных интересов корпорации от внутренних и внешних угроз.

В результате обобщения и критического осмысления имеющихся в экономической литературе предложений по построению системы показателей безопасности предложена следующая система показателей оценки уровня информационной безопасности:

– попытки несанкционированного доступа к корпоративным сетям со стороны конкурентов или криминальных структур;

– попытки несанкционированного доступа к внутрикорпоративным сетям со стороны сотрудников, не имеющих допуска;

– утечка информации на электронных и бумажных носителях в результате нарушения сотрудниками корпорации инструкций по обеспечению информационной безопасности;

– контакты сотрудников корпорации с представителями конкурентов или криминальных структур;

**Список использованной литературы**

1. Закон Республики Казахстан от 6 января 2012 г. № 527-IV «О национальной безопасности Республики Казахстан» (с изменениями по состоянию на 10.07.2012 г.) // Казахстанская правда. — 2012 г. — 17 янв. — № 19-20 (26838-26839).
2. Указ Президента Республики Казахстан от 14 ноября 2011 г. № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года» // Электронная база нормативно-правовых актов «Законодательство».
3. Постановление Правительства Республики Казахстан от 30 сентября 2011 г. № 1128 «О проекте Указа Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан до 2016 года» (утвержден) // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz/ (дата обращения 26.08.2016)
4. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 c.
5. Баймакова, И.А.. Обеспечение защиты персональных данных– М.: Изд-во 1С-Паблишинг, 2010. – 216 с.