**Разработка сценариев реализации угроз и их публикация.**

1. Постановка проблемы
   1. Профессиональная ситуация: Разработка сценариев реализации угроз и их публикация.
   2. Описание ситуации:

Угрозы возникают из противоречий экономических интересов различных элементов, взаимодействующих как внутри, так и вне социально-экономической системы — в том числе и в информационной сфере. Они и определяют содержание и направления деятельности по обеспечению общей и информационной безопасности. Следует отметить, что анализ проблем экономической безопасности необходимо проводить, учитывая взаимосвязи экономических противоречий, угроз и потерь, к которым может приводить реализация угроз. Такой анализ приводит к следующей цепочке:

* источник угрозы (внешняя и/или внутренняя среда предприятия)
* зона риска (сфера экономической деятельности предприятия, способы её реализации, материальные и информационные ресурсы)
* фактор (степень уязвимости данных, информации, программного обеспечения, компьютерных и телекоммуникационных устройств, материальных и финансовых ресурсов, персонала
* угроза (вид, величина, направление)
* возможность её реализации (предпосылки, объект, способ действия, скорость и временной интервал действия)
* последствия (материальный ущерб, моральный вред, размер ущерба и вреда, возможность компенсации).

Анализ негативных последствий возникновения и осуществления угроз предполагает обязательную идентификацию возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации. В связи с этим угрозы экономической и информационной безопасности необходимо классифицировать с тем, чтобы наиболее полно и адекватно проводить указанную идентификацию: по источнику угрозы, по природе возникновения, по вероятности реализации, по отношению к виду человеческой деятельности, по объекту посягательства, по последствиям, по возможностям прогнозирования.

В ходе анализа необходимо убедиться, что большинство возможных источников угроз и уязвимости идентифицированы и сопоставлены друг с другом, а всем идентифицированным источникам угроз и уязвимостям сопоставлены методы их нейтрализации и устранения.

Указанная классификация может служить основой для выработки методики оценки актуальности той или иной угрозы, и при обнаружении наиболее актуальных угроз могут приниматься меры по выбору методов и средств для их предотвращения или нейтрализации.

При выявлении актуальных угроз экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

Благодаря созданию сценариев реализации угроз возможно отследить цель неправомерных действий и технические средства ее достижения.

* 1. Задача:

Провести анализ этичности разработки сценариев реализации угроз и их публикация внутри компании.

1. Оценка ситуации с точки зрения профессиональной этики:

Разработка сценариев реализации угроз и их дальнейшая публикация внутри компании сама по себе не противоречит законодательству. С точки зрения кодекса профессиональной этики эта ситуация конкретно не рассматривается. Наибольшую угрозу для Информационной Безопасности представляют внутренние факторы. Таким образом, публикацию таких сценариев внутри компании можно рассматривать как памятку сотрудникам компании, которая уменьшит количество критичных ошибок сотрудников. Соответственно, с точки зрения кодекса профессиональной этики, это идет на пользу профессионализма сотрудников. Следовательно, данная ситуация является полностью этичной.

1. Моделирование последствий решения:

После разработки сценариев реализации угроз следует их анализ. В процессе анализа есть возможность выявить наиболее важные для Информационной Безопасности сценарии и предотвратить их развитие. Вопрос о том, будут ли дальнейшие действие о предотвращении этих сценариев этичными или нет в данном вопросе не рассматриваются.

Если внутри компании находятся недоброжелатели, то публикация таких сценариев может нанести урон компании, поэтому важно вовремя проводить воспитательные работы с сотрудниками, улучшать систему приема на работу.

1. Оценка возможности существования альтернативных решений:

Так как основную задачу, которую решает публикация сценариев реализации угроз – это увеличение уровня профессионализма сотрудников, то очевидным альтернативным решением является организация обучения сотрудников и их аттестация на знание технологий работы с информацией и механизмов ее защиты.