Риск - это деятельность, связанная с преодолением неопределенности в ситуации неизбежного выбора, в процессе которого имеется возможность количественно и качественно оценить вероятность достижения предполагаемого результата, неудачи и отклонения от цели.

Как нами уже было отмечено ранее, основным этапом жизненного цикла в рамках данного проекта выступает разработка самой АИС. При этом можно выделить следующие риски:

- риск персонала и проектных коммуникаций;
- технический и программный риски.

Основными факторами возникновения первого риска являются:

- зависимость от ключевого персонала;
- увольнение ключевых сотрудников, что повлечет за собой потери для проекта в виде знаний и информации, собранной данными сотрудниками;
- недопонимание между участниками проекта из-за отсутствия налаженной системы коммуникаций и поэтапного документирования работ;
- неправильное понимание задач проектирования программистами, в связи с чем неправильная реализация проекта;
- привлечение программистов без достаточного опыта работы с системами подобного класса.

Основными мерами предотвращения этого служит:

- тщательный отбор персонала, задействованного в данном проекте, обеспечение сертификации, а также организация контроля деятельности персонала их руководителями;
- разделение обязанностей, наличие резерва на выдвижение, обучение перспективных сотрудников, а также документирование накопленных знаний;
- налаженная система коммуникаций между сотрудниками проекта, подробное и четкое документирование требований и доступность проектной документации всем участникам рабочей группы.

Технический и программный риски могут породить:

- частичную или полную приостановку этапа разработки из-за ошибок в используемом программном обеспечение. Последствиями данного риска также может быть частичная или полная потеря созданной на данном этапе информации в виде кода программы;
- контрольный пример не учитывает всех особенностей системы, то есть недостаточно проработан, что может привести к ошибкам на этапе эксплуатации системы;
- документация по системе не включает в себя подробного описания всего функционала системы, что в дальнейшем может привести к возникновению трудностей не этапе эксплуатации.

Этого можно избежать, учитывая:

- использование только проверенного лицензионного программного обеспечения, а также производить регулярное резервное копирование данных на
  альтернативные источники хранения данных;
- привлечение к тестированию опытных специалистов, многократные проверки и прогоны работоспособности системы для выявления малейших неисправностей в ходе работы;
- проверка документации перед передачей системы заказчику, контроль ее ведения и составления на протяжение всех этапов жизненного цикла ИС.

В процессе внедрения могут возникнуть такие риски, как:

- ○ Риск персонала;
  ○ Технический риск.

Факторами первого риска являются:

- увеличение нагрузки на персонал;
- несогласованность действий персонала исполнителя и сотрудников предметных областей;
- трудности с обучением персонала заказчика из-за нежелания работать с новой системой;
- отсутствие поддержки внедрения ИС со стороны отдельных ключевых участников проекта;

- неучастие руководителей высшего звена в проекте. Этого можно избежать, путем реализации следующих идей:
- проведение обучения персонала заказчика работы с системой;
- составление плана внедрения ИС;- доведение до персонала заказчика смысла внедрения автоматизированной системы;
- активное вовлечение высшего руководства в проект, активное взаимодействие с ним в ходе проекта и своевременное принятие решений, необходимых для нормальной реализации проекта.

Основными факторами технического риска являются следующие:

1. потеря данных при внедрении ИС;
2. возможный отказ технического оборудования при внедрении ИС.

Мерами предупреждения этого служит:

- привлечение квалифицированных технических специалистов, работающих ранее с проектами внедрения ИС, а также их активная работа с техническими специалистами исполнителя;
- использование пилотного, поэтапного - подхода к организации внедрения.

В процессе эксплуатации и сопровождения разработанной ИС могут возникнуть:

- технические риски;
- риски персонала. Факторами технических рисков являются:
- ошибки в программе вызывающие простой системы;
- невозможность осуществления требуемых действия, «зависание» программы;
- использование вредоносных программ (вирусы, черви, трояны, логические бомбы), использование в корыстных целях найденных ошибок (дыр) в программах, перехват информации по телекоммуникациям, воровство информации;
- некорректная эксплуатация оборудования;
- приостановка деятельности третьего лица (например, провайдера Интернет услуг), что повлечет за собой невозможность передачи отчетов из филиалов и контроля деятельности филиалов;
- несоответствие функциональных возможностей системы бизнес-процессам в комплекса задач в следствие реорганизационных изменений.

Предотвратить данные обстоятельства можно, соблюдая следующие моменты:

- тщательное тестирование и выявление ошибок на этапе разработки;
- устранять в кратчайшие сроки ошибки силами прошедших подготовку на этапе внедрения технических специалистов;
- администратор сети должен следить за безопасностью информации, использовать и вовремя обновлять антивирусные программы, правильно настроить FireWall, которые будут разделять локальную и внешнюю сеть, предоставить работникам организации возможность работы только с той информацией, которая им необходима для исполнения своих служебных обязанностей;
- разделение клиентского и серверного оборудования, а также необходимо привлечение обученного работе с системой квалифицированного персонала;
- наличие альтернативных средств доступа в Интернет или других способов передачи данных;
- документирование технических условий и их согласование со всеми заинтересованными участниками проекта;
- обязательное утверждение любых изменений.

Факторами возникновения риска персонала являются следующие

обстоятельства:

- нарушение информационной безопасности работы - возможна утечка информации из-за злоумышленных действий сотрудников и не желании работать с новой системой;
- не определен этап выхода их проекта консультантов заказчика.

В противовес этому может выступать:

- организация системы поощрений использующего систему персонала заказчика;
- прием на работу сотрудников при условии не разглашения коммерческой тайны в противном случая - применение штрафных санкций;
- четкое планирование сроков проекта и момента прекращения работы над проектом со стороны исполнителя.

Таким образом, нам удалось определить основные риски, которые могут возникнуть на каждом из этапов жизненного цикла информационной системы, определить факторы их возникновения, а также привести рекомендации по их предотвращению.