Image not found or type unknown

Темпы развития современных информационных технологий (ИТ) и построенных на их основе информационных систем (ИС) значительно опережают темпы разработки рекомендаций и нормативно-правовой базы оценки рисков на различных этапах жизненного цикла. Таким образом, возникает актуальная задача оценки уровня безопасности информационной системы, которая связанных с оценкой рисков: по каким критериям проводить оценку эффективности защиты, как оценивать риски? Вследствие этого, дополнительно к требованиям рекомендаций и нормативно-правовых документов, приходится адаптировать к нашим условиям и применять методики международных стандартов, а также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности обеспечения безопасности и защиты информации в информационных системах на различных этапах жизненного цикла.

В дальнейшем исследовании будем опираться на модель жизненного цикла информационной системы, представленной на рис. 1.

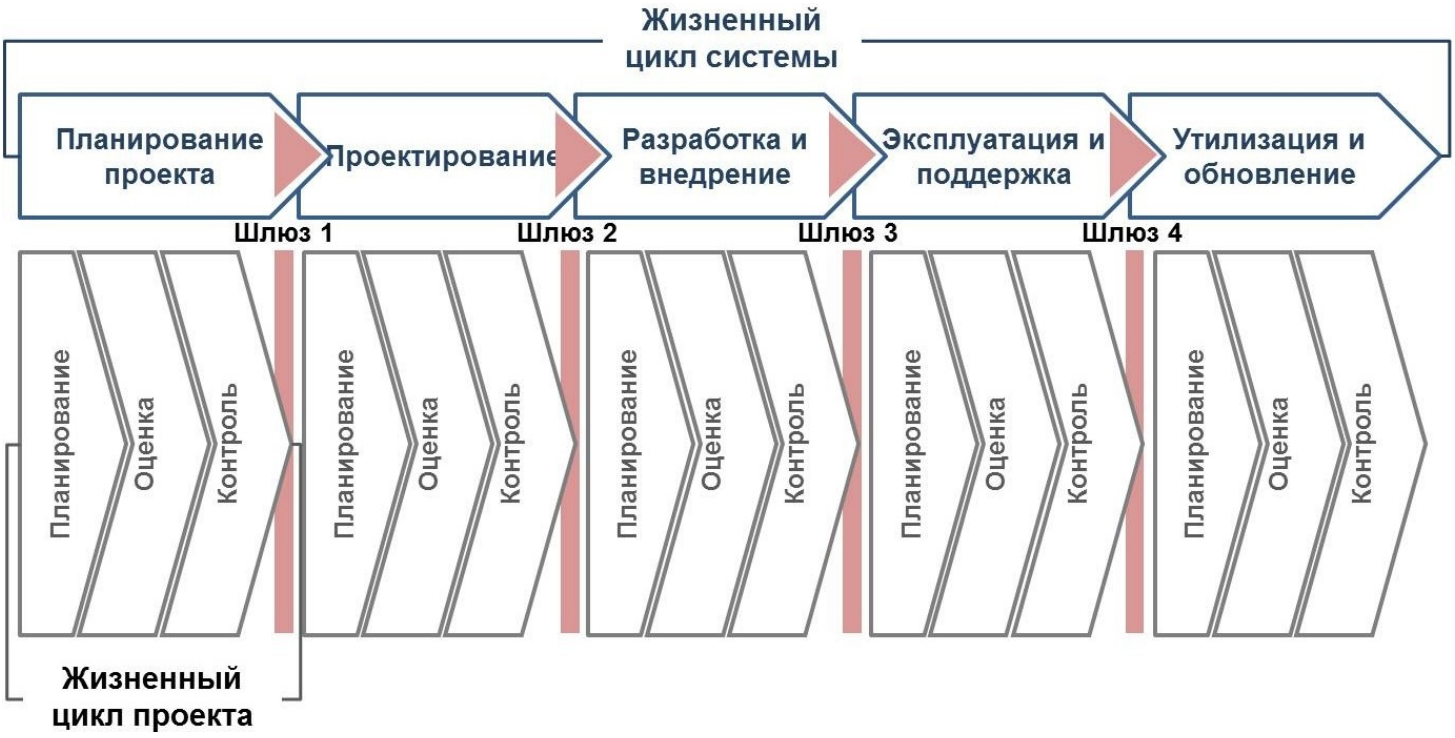

Рисунок 1 – Модель жизненного цикла информационной системы, принятая для исследования

Обращаясь к последним работам отечественных и зарубежных специалистов по оценки рисков в ИТ-проектах, ИС и процессах автоматизации, необходимо отметить тот факт, что современные методы (исходя из этапа жизненного цикла ИС) должны позволять:

- оценить риски создания ИС, определить актуальность ее создания *(на этапе планирования проекта)*;

- рассчитать и экономически обосновать размер необходимых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести затраты на обеспечение безопасности с потенциальным убытком и вероятностью его возникновения *(на этапе проектирования проекта)*;

- выполнить количественную оценку уровня безопасности ИС, задать допустимые уровни рисков, разработать план мероприятий по обеспечению необходимого уровня безопасности на организационно-управленческом и техническом уровнях с использованием современных методик и средств *(на этапе разработки и внедрения)*;

- определять функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению системы управления рисками, создать необходимую подсистему *(на этапе разработки и внедрения)*;

- выявлять и проводить первоочередное блокирование наиболее опасных уязвимостей к осуществлению атак на критические информационные ресурсы *(на этапе эксплуатации и поддержки)*;

- обеспечить поддержку введенного комплекса управления рисками в соответствии с условиям работы ИС, обеспечение модификации технологических процессов и технических средств защиты *(на этапе эксплуатации и поддержки)*;

- оценка рисков при принятии решения об утилизации и обновлении ИС (*на этапе утилизации и обновления*).

Условно все используемые методики оценки рисков можно разделить на три категории, основные плюсы и минусы которых рассмотрены в приведенной ниже табл. 1.

Таблица 1 – Методы оценки рисков

Категория методик	Характеристика методик	Примеры	Позитивные качества	Негативные качества
1	2	3	4	5
Статистические	Базируются на анализе массивов статистических данных и моделирования с использованием методов математической статистики и теории вероятности	Value-at-risk, Cash-flow-at-risk	Высокая точность расчетов, возможность моделирования скотобоец сценариев, измеренные показатели, частичная стандартизация	Высокие затраты на информацию и проведение анализа, риск адекватности полученной модели
Аналитические	Базируются на сборе и объективном анализе информации, а также принятии решения, исходя из комплексного анализа как количественных так и качественных показателей.	Рейтинговые методики, финансовый анализ	Возможность индивидуального набора показателей для анализа, широкое применение, возможность достижения объективной оценки при небольшой стоимости	Определенный субъективизм оценок, не всегда измеряемые показатели (финансовая оценка риска), отсутствие стандартов

Категория методик	Характеристика методик	Примеры	Позитивные качества	Негативные качества
1	2	3	4	5
Экспертные	Основываются на субъективном анализе количественных и качественных показателей с использованием	Инженерные оценки. Ранжирование рисков	Низкая скорость получения результатов, необходимость сбора большого объема информации	Высокая зависимость от человеческого фактора (эксперта), трудности в получении финансовой оценки риска

Как видно из приведенной табл. 1, наиболее дешевым и быстрым методом оценки являются экспертные методики, когда за счет опрашивания одного или нескольких экспертов, можно получить общую оценку того или другого риска. Тем не менее, следует отметить, что универсальных методик не существует, поскольку даже такие стандартные приемы как VAR-анализ требуют модификации относительно каждой конкретной ИС и ее назначения.

Методика проведения аналитических работ по оценки рисков и синтеза системы управления рисками должна позволять:

- проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности ИС;

- избегнуть затрат на лишние мероприятия безопасности, возможные при субъективной оценке рисков;

- предоставлять помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла ИС;

- обеспечить проведение работ в сжатые сроки;

- представить обоснование для выбора мер противодействия;

- оценить эффективность контрмер и сравнить их разные варианты.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы ИС, для которых в дальнейшем будут получены оценки рисков. При этом нужно разделить рассмотренные ресурсы и внешние элементы, с которыми осуществляется взаимодействие.

Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные. Примерами внешних элементов являются сети связи и т.п. При построении модели будут учитываться взаимодействия между ресурсами. Например, выход из строя какого-нибудь оборудования может привести к потере информации или выхода из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения информационной безопасности.

Построим онтологическую модель рисков ИС на различных этапах ее жизненного цикла, которая выделяет риски как явление в целом, а также общие механизмы защиты от них.

Источник

угрозы

Потенциальные

угрозы

Неблагоприятное событие

Работа ИС

Заданные показатели

Качество планирования

Возможность реализации

Уровень негативных последствий

Условия реализации

Эффективность

ИС

Уровень разрушения

РИСК

Уровень приемлемого риска

Лицо, принимающее решение

Стратегия защиты

Принятие

риска

Предотвращение

риска

Снижение риска

Порождает

Использует

Имеет

Трансформируется

Повреждает

Обладает

Обеспечивает

Определяет

Имеет

Определяет

Сравнивается

Устанавливает

Выбирает

Заинтересован в улучшении

Снижает уровень

Уклонение

Ликвидация

Корректировка

Подвергается

Оценивает

Рисунок 2 – Онтологическая модель оценки и управления рисками информационной системы

Выводы.

1) Риски существуют на всех этапах жизненного цикла ИС - от начала их создания, к прекращению эксплуатации.

2) Задача управления рисками состоит в уменьшении влияния нежелательных факторов на жизненный цикл ИС для получения результатов ближайших к желательным.

3) Возможности маневрирования во время управления рисками довольно разнообразные: предотвращение риска, отклонение от риска, сознательное и неосознанное принятия риска, дублирование операций, объектов или ресурсов, сокращение величины потенциальных и фактических потерь, распределение риска, разукрупнение риска, разнесение экспозиций в пространстве и во времени, изоляция опасных синергетических факторов друг от друга, перенесение риска на других агентов.

4) Независимо от выбора метод управления риском, вообще устранить риск не удастся, ведь в произвольной ИС всегда существует определенный уровень остаточной энтропии.

5) Оценка риска является достаточно сложным процессом, который обладает развитой методологической базой, применяемой на различных этапах жизненного

цикла ИС.

Список использованной литературы.

1. Гагарина Л.Г. Разработка и эксплуатация автоматизированных информационных систем. Учебное пособие. – М.: Форум, Инфра-М, 2015. – 384 с.

2. Ерохин В.В., Погонышева Д.А., Степченко И.Г. Безопасность информационных систем. Учебное пособие. – М.: Флинта, Наука, 2015. – 184 с.

3. Атисков А. А. Онтологическое проектирование для анализа политик безопасности. – М.: LAP Lambert Academic Publishing, 2014. – 68 с.

4. Песоцкая Е.А. Управление рисками ИТ. – М.: LAP Lambert Academic Publishing, 2011. – 184 с.

5. Скабцов Н.А. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.

6. Брумштейн Ю.М., Тарков Д.А., Дюдиков И.А. Анализ моделей и методов выбора оптимальных совокупностей решений для задач планирования в условиях ресурсных ограничений и рисков // Прикаспийский журнал: управление и высокие технологии. – 2013. – № 3. – С. 169-179.