УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ И «УРОВЕНЬ ЗРЕЛОСТИ» КОРПОРАТИВНЫХ СИСТЕМ

Исламова Дилдора Султаноавна
старший преподаватель «Оптические системы связи и сетевая безопасность» Каршинского филиала ТУИТ им. Мухаммада ал-Хоразми

Аннотация: *Опасности или риски рассматриваются как один из важных факторов, негативно влияющих на успех информационных систем. Неспособность должным образом организовать управление рисками может поставить под угрозу производительность и результаты каждой корпоративной информационной системы. Управление любым проектом – это комплексный процесс взаимосвязанных отношений и информационных потоков. В данной статье изучены основные инструменты выявления и исследования ряда проблем, возникающих при обеспечении информационной безопасности в корпоративных информационных системах и рисков, оказывающих негативное влияние на развитие бизнеса предприятия, а также основные сведения об их «зрелости» показаны уровни реализации проекта.*

Ключевое слова: *риск, корпоративные информационные системы, информационные риски, информационные сети.*

INFORMATION RISK MANAGEMENT AND “MATURITY LEVEL” OF CORPORATE SYSTEMS

Islamova Dildora Sultanoavna
Senior lecturer "Optical Communication Systems and Network Security" of the Karshi Branch of TUIT named after Muhammad al-Khwarizmi

Abstract: *Dangers or risks are considered as one of the important factors that negatively affect the success of information systems. Failure to properly manage risk can compromise the performance and results of every enterprise information system. Managing any project is a complex process of interconnected relationships and information flows. This article examines the main tools for*

identifying and researching a number of problems that arise when ensuring information security in corporate information systems and risks that have a negative impact on the development of the enterprise's business, as well as basic information about their "maturity" and shows the levels of project implementation.

Key words: *risk, corporate information systems, information risks, information networks.*

Основным фактором, определяющим отношение организации к вопросам информационной безопасности, является степень ее «зрелости». В соответствие с моделью предложенной Carnegie Mellon University выделяется пять уровней зрелости, которым соответствует различное понимание проблем управления информационными рисками организации.

Постановка и решение задачи управления информационными рисками для организаций, находящихся на разных уровнях зрелости будут различными.

Уровень 1 - «Анархия». Признаки:

– сотрудники сами определяют, что хорошо, а что плохо;
– затраты и качество не прогнозируются;
– отсутствует контроль изменений;
– высшее руководство плохо представляет реальное положение дел.

Характеристики организации в области информационной безопасности:

– политика в области информационной безопасности не формализована и руководство этими вопросами не занимается;
– обеспечением информационной безопасности сотрудники могут заниматься по собственной инициативе, в соответствии со своим пониманием задач;

Таким образом, на первом уровне задача управления информационными рисками формально не ставится, поскольку с точки зрения руководства организации, находящейся на первом уровне зрелости, эти задачи, как

правило, не актуальны. Но это не значит, что она не решается сотрудниками по собственной инициативе, и возможно эффективно, поэтому организации могут быть вполне жизнеспособными.

Уровень 2 - «Фольклор». Признаки:

– выявлена определенная повторяемость организационных процессов;

– опыт организации представлен в виде преданий корпоративной мифологии;

– знания накапливаются в виде личного опыта сотрудников и пропадают при их увольнении.

Характеристики организации в области информационной безопасности:

– на уровне руководства существует определенное понимание задач обеспечения управления информационными рисками;

– существуют стихийно сложившиеся процедуры обеспечения информационной безопасности, их полнота и эффективность не анализируется;

– процедуры не документированы и полностью зависят от личностей, вовлеченных в них сотрудников;

– руководство не ставит задач формализации процедур управления информационными рисками.

Таким образом, на втором уровне проблема управления информационными рисками решается неформально, на основе постепенно сложившейся практики. Комплекс контрмер (организационных и программно-технических) позволяет защититься от наиболее вероятных угроз, как потенциально возможных, так и имевших место ранее. Вопрос относительно эффективности защиты не ставится.

Уровень 3- «Стандарты». Признаки:

– корпоративная мифология записана на бумаге;

– процессы повторяемы и не зависят от личных качеств исполнителей;

– информация о процессах для измерения эффективности не собирается;

– наличие формализованного описания процессов не означает, что они работают;
– организация начинает адаптировать свой опыт к специфике бизнеса;
– проводится знаний и умений сотрудников с целью определения необходимого уровня компетентности;
– вырабатывается стратегия развития компетентности.

Характеристики организации в области информационной безопасности:

– руководство осознает задачи в области управления информационными рисками;
– в организации имеется документация (возможно неполная), относящейся к политике информационной безопасности:
– руководство заинтересовано в исполнении стандартов в области информационной безопасности, оформлении документации в соответствии с ними;
– осознается задача управления информационными рисками на всех стадиях жизненного цикла информационно-коммуникационной технологии.

Таким образом, на третьем уровне в организации считается целесообразным следовать в той или иной мере (возможно частично) стандартам и рекомендациям, обеспечивающим базовый уровень информационной безопасности (например, ISO/IEC 27001), вопросам документирования уделяется должное внимание. Анализ рисков рассматривается как один из элементов технологии управления информационными рисками на всех стадиях жизненного цикла. Понятие риска включает несколько аспектов: вероятность, угроза, уязвимость, иногда стоимость.

Технология управления информационными рисками в полном варианте включает следующие элементы:

– документирование КИС с позиции информационной безопасности;

– категорирование информационных ресурсов с позиции руководства организации;

– определение возможного воздействия различного рода происшествий в области информационной безопасности на информационно-технологические - и бизнес-процессы;

– анализ информационных рисков;

– технология управления информационными рисками на всех этапах жизненного цикла КИС;

– аудит в области информационных рисков.

Уровень 4- «Измеряемый». Признаки:

– процессы измеримы и стандартизованы.

Характеристики организации в области информационной безопасности:

– имеется полный комплект документов, относящийся К обеспечению режима информационной безопасности, оформленный в соответствии с каким-либо стандартом;

– действующие инструкции соблюдаются, документы служат руководством к действию соответствующих должностных лиц;

– регулярно проводится внутренний (и возможно внешний) аудит и анализ информационных рисков;

– руководство уделяет должное внимание вопросам управления информационными рисками, в частности, имеет адекватное представление относительно существующих уровней информационных угроз и уязвимостей, потенциальном ущербе (потерях) в случае возможных инцидентов.

Таким образом, на четвертом уровне для руководства организации актуальны вопросы измерения параметров, характеризующих режим информационной безопасности. На этом уровне руководство осознанно принимает на себя ответственность за выбор определенных величин

остаточных рисков (которые остаются всегда). Риски, как правило, оцениваются по нескольким критериям (не только стоимостным).

Технология управления информационными рисками остается прежней, но на этапе анализа рисков применяются количественные методы, позволяющие оценить параметры остаточных рисков, эффективность различных вариантов контрмер при управлении рисками.

Уровень 5 - «Оптимизируемый». Признаки:

– фокус сосредотачивается на повторяемости, измерении эффективности и оптимизации;

– вся информации о функционировании процессов фиксируется.

Характеристики организации в области информационной безопасности:

– руководство заинтересовано в количественной оценке существующих информационных рисков, готово нести ответственность за выбор определенных уровней допустимых и остаточных информационных рисков, ставит оптимизационные задачи построения системы управления информационными рисками.

Таким образом, на пятом уровне ставятся и решаются различные варианты оптимизационных задач в области управления информационными рисками. Примеры постановок задач:

– выбрать вариант системы управления информационными рисками, оптимизированной по критерию стоимость/эффективность при заданном уровне остаточных рисков;

– выбрать вариант системы управления информационными рисками, при котором минимизируются остаточные риски при ее фиксированной стоимости;

– выбрать архитектуру системы управления информационными рисками с минимальной стоимостью владения на протяжении жизненного цикла при определенном уровне остаточных рисков.

Результаты исследования, что в настоящее время более половины организаций относятся к первому или второму уровню зрелости. Организаций третьего уровня зрелости около 40% от общего числа и только порядка 7% от общего числа организации, относятся к четвертому и пятому уровням зрелости.

Использованная литература

1. Филатов, А. А. (2020). Управление информационными рисками в организации. Молодой ученый, (21), 199-202.
2. Лех, Д. Ю., Легкий, В. Н., & Ющенко, В. П. (2022). ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. In Наука Промышленность Оборона (pp. 268-272).
3. Sultanovna, I. D. (2022). KORXONA AXBOROT TIZIMLARINI BOSHQARISHDA AXBOROT XAVFSIZLIGI PARAMETRLARINING USTIVORLIGI. In *E Global Congress* (No. 1, pp. 28-30).
4. Пардаев, О. (2023). МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЦИФРОВОЙ ТРОНСФОРМАЦИИ В НАРОДНОМ ОБРАЗОВАНИИ. *Innovations in Technology and Science Education*, *2*(11), 37-42.
5. Мухитдинов, Х. С., & Худоёров, Л. Н. (2016). РАЗРАБОТКА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И ПРОГНОЗИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ. Наука и мир, (7-1), 54-56.
6. Бекматов А.К., Кутдусова Э.Р., Мукимов Ш.И., & Давлатова Н.Н. (2023). ПРОГРЕССИВНЫЕ ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Экономика и социум, (6-1 (109)), 1264-1270.
7. Бекматов, А. К., Кутдусова, Э. Р., & Мукимов, Ш. И. (2023). ПРЕИМУЩЕСТВА И ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОЦИАЛЬНО-

ЭКОНОМИЧЕСКОЙ СФЕРЕ. O'ZBEKISTONDA FANLARARO INNOVATSIYALAR VA ILMIY TADQIQOTLAR JURNALI, 2(20), 280-286.