УДК 004.02

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ОЦЕНКИ РИСКА В ЦЕЛЯХ ОПРЕДЕЛЕНИЯ ЭФФЕКТИВНОСТИ ПРИНЯТЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

Диченкова В. (Университет ИТМО)
Научный руководитель - профессор (квалификационная категория "профессор практики"), доктор технических наук, Лившиц И.И. (Университет ИТМО)

По данным национальных регуляторов в области информационной безопасности, на многих предприятиях вопрос обеспечения информационной безопасности реализован не в соответствии с утвержденной документацией. Проблема заключается в том, что система защиты информации воспринимается как навязанное требование, неисполнение которого не повлечет за собой неисправимых последствий. Предлагается методика, неотъемлемой частью которой является оценка рисков (остаточных рисков), наглядное представление необходимости затрат на создание экономически эффективной системы защиты информации, порядок реализации и контроля эффективности применяемых мер защиты информации.

Введение. По данным национальных регуляторов в области информационной безопасности на многих предприятиях вопрос обеспечения информационной безопасности реализован не в соответствии с утвержденной документацией. Иными словами, реальные меры по защите информации применяются либо формально (пароль есть, но его легко подобрать по словарю, антивирус установлен, но выключен пользователем), либо не применяются совсем, как следствие – эффективность системы защиты информации фактически оказывается значительно ниже ожидаемой. Проблема заключается в том, что система защиты информации воспринимается как навязанное излишнее требование, неисполнение которого не повлечет за собой неисправимых последствий лично для высшего руководства. Как одно из решений в данной работе предлагается внедрение в процесс создания и сопровождения системы защиты информации менеджмента рисков (остаточных рисков).

Основная часть. В настоящий момент управление рисками в отношении большей части сфер применения информационных технологий установлено только как рекомендации. Предлагается добавить в процесс создания, внедрения, оценивания и непрерывного улучшения системы защиты информации – управление рисками (остаточными рисками).

Необходимость применения процессного риск-ориентированного подхода при создании систем защиты информации отражена в работах, посвященных проблемам анализа риска на критически значимых объектах [1], методам оценки рисков информационной безопасности корпоративных информационных систем [2] и кредитно-финансовых организаций [3]. В процессе исследования выявлена проблема не только недостаточного внимания к реализации и контролю обеспечения безопасности информации со стороны руководства, но и отсутствие персональной ответственности персонально высшего менеджмента и, соответственно, сотрудников в области информационной безопасности. Система защиты информации воспринимается как объект, требующий затрат и не обеспечивающий прибыли, однако не принимается во внимание тот факт, что при грамотном подходе к созданию системы защиты информации минимизируются такие последствия инцидентов, как потеря (рабочего) времени, упущение бизнес возможностей, невыполнение договоров, штрафы за неисполнение государственного законодательства в области защиты информации, затраты на нейтрализацию инцидента (привлечение дополнительных кадров), репутационные и иные потери, связанные с "неосязаемым капиталом" [4].

Предлагается методика, неотъемлемой частью которой является оценка рисков, наглядное представление необходимости затрат на создание системы защиты информации, порядок реализации и контроля эффективности мер защиты информации.

Выводы. Методика позволяет охватить широкий спектр факторов влияния на процесс принятия решений при создании систем защиты информации и предоставляет возможность объективного детального объяснения, руководствуясь диаграммами принятия решений. По результатам применения методики владелец информационной системы будет также располагать достоверной объективной информацией о количественной модели оценки рисков, которая покажет текущее положение дел относительно безопасности информации и о модели для будущего пересмотра ценности активов, анализа рисков (остаточного риска) и улучшения деятельности по защите информации.

Список использованных источников:

1. Сидорин В.В., Антонов А.В. Концептуальная модель и метод менеджмента критически значимых рисков // Организатор производства. – 2021. – Т.29 № 2. – С. 39–53.
2. Беззатеев С.В., Елина Т.Н., Мыльников В.А., Лившиц И.И. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т.21. № 4. – С. 553-561.
3. Беляев Е.А., Емельянова О.А., Лившиц И.И. Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т.21 № 3. – С. 437-441.
4. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности. – М.: Стандартинформ, 2011. – С. 51.

Диченкова В. (автор) _____
Подпись

Лившиц И.И. (научный руководитель) _____
Подпись