СИСТЕМНЫЙ АНАЛИЗ ДЛЯ ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ

Е.В. Бегляк, Е.А. Лещенко, А.В. Луцкий
Научные руководители –
Алексеев В.Ф., к.т.н., доцент
Пискну Г.А., к.т.н., доцент
Белорусский государственный университет информатики и радиоэлектроники

Проблема принятия решений в условиях неопределенности в области информационной безопасности становится все более важной, учитывая непредсказуемые вероятности и последствия событий в постоянно меняющемся ландшафте киберугроз. Одной из таких угроз может быть и воздействие электромагнитного импульса [1].

Системный анализ один из самых эффективных инструментов, которые может использовать предприятие, чтобы распознавать угрозы, связанные с безопасностью. Использование системного анализа для определения угроз безопасности помогает выявлять уязвимости и налаживать контроль за безопасностью в компаниях [1–7].

Системный анализ может помочь определить уязвимости и угрозы безопасности в системе. Он включает в себя анализ функций, структуры и процессов системы, а также ее взаимодействия с окружающей средой. Для того чтобы выполнить системный анализ, необходимо определить цели, задачи и ограничения проведения анализа.

Важно учитывать, что реализация безопасности системы является одним из главных вопросов, при выполнении системного анализа. В первую очередь, необходимо оценить риски и определить уязвимости системы.

Применение системного анализа позволяет определить факторы, влияющие на производительность и надежность системы, а также выявить угрозы безопасности и возможные пути их решения. Для этого необходимо провести анализ данных, проанализировать существующие угрозы и уязвимости, а также разработать стратегию повышения безопасности системы.

Применяя структурированный и методичный подход к анализу угроз, специалисты по безопасности лучше оснащены для выявления потенциальных уязвимостей и разработки эффективных стратегий по их снижению. Одним из ключевых преимуществ использования системного подхода является то, что он позволяет аналитикам целостно взглянуть на безопасность, учитывая такие факторы, как бизнес-цели организации, технологическая инфраструктура и соответствующие нормативные требования. Такой комплексный подход помогает обеспечить эффективность и долгосрочную устойчивость разработанных стратегий по снижению рисков. Кроме того, используя инструменты и методы, основанные на данных, такие как алгоритмы машинного обучения и передовые аналитические платформы, аналитики могут выявлять

закономерности и тенденции в деятельности угроз, которые в противном случае могут быть не очевидны. Это позволяет им предвидеть и реагировать на возникающие угрозы до того, как они смогут причинить вред. В конечном итоге, включив систематический анализ в свои программы безопасности, организации могут более эффективно управлять рисками и защищать свои критически важные активы.

Системный анализ потенциальных угроз безопасности включает в себя ряд шагов, направленных на выявление потенциальных рисков безопасности, оценку их влияния и определение оптимального курса действий по их снижению. Рассмотрим основные шаги, которые необходимо предпринять при проведении системного анализа угроз безопасности:

– *определение проблемы* – включает в себя определение масштаба проблемы и выявление проблемных областей. Важно собрать все необходимые данные и информацию для полного понимания проблемы;

– *анализ проблемы* – на этом этапе необходимо проанализировать собранные данные и информацию, чтобы выявить первопричину проблемы;

– *разработать потенциальные решения* – этот этап включает в себя разработку потенциальных решений выявленной проблемы. Важно рассмотреть все возможные решения, определив их плюсы и минусы;

– *оценить потенциальные решения* –этап включает в себя оценку каждого решения и определение наилучшего курса действий. Важно учитывать такие факторы, как осуществимость, стоимость и потенциальное влияние каждого решения;

– *реализовать решение* – этап включает в себя внедрение выбранного решения и мониторинг его эффективности в течение определенного времени.

Следуя этим шагам, организации могут эффективно использовать системный анализ для выявления и предотвращения потенциальных угроз безопасности.

Системный анализ является важнейшим шагом в выявлении угроз безопасности и реализации эффективных мер по их снижению. Придерживаясь системного подхода, организации могут комплексно и эффективно устранять потенциальные риски безопасности.

Библиографический список

1. Моделирование угроз в условиях методической неопределенности: [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/publications/reports/2018/12/11/modelirovanie-ugroz-v-usloviyakh-metodichskoy-neopredelennosti/. (Дата обращения: 30.10.2023).

2. Оценка качества передачи информации в системе диспетчеризации на базе MQTT-архитектуры / В. Ф. Алексеев [и др.] // BIG DATA and Advanced Analytics = BIG DATA и анализ высокого уровня : сборник научный статей VIII Международной научно-практической конференции, Минск, 11-12 мая 2022 года / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: В. А. Богуш [и др.]. – Минск, 2022. – С. 483–488.

3. Алексеев, В. Ф. Испытание электронных средств по моделям воздействия электростатического разряда / В. Ф. Алексеев, Г. А. Пискун, Н. А. Панасюк // Сучасні виклики і актуальні проблеми науки, освіти та

виробництва: міжгалузеві диспути: матеріали XV міжнародної науково-практичної інтернет-конференції, Київ, 29 квітня 2021 р. / Наукова платформа Open Science Laboratory. – Київ, 2021. – С.284–293.

4. Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы: [Электронный ресурс]. URL: https://arinteg.ru/articles/analiz-ugroz-informatsionnoy-bezopasnosti-27291.html. (Дата обращения: 30.10.2023).

5. Бразевич, Д. Анализ проблем обеспечения информационной безопасности в условиях современного общества / Д. Бразевич [и др.] // Открытый журнал социальных наук – №8, 2020. – С.231-241. DOI: 10.4236/jss.2020.82018.

6. Теоретические аспекты разработки образовательной информационной среды подготовки ИТ-специалиста / В. Ф. Алексеев [и др.] // BIG DATA and Advanced Analytics = BIG DATA и анализ высокого уровня : сборник научный статей VIII Международной научно-практической конференции, Минск, 11-12 мая 2022 года / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: В. А. Богуш [и др.]. – Минск, 2022. – С. 425–430.

7. Статистика DDoS-атак в первом квартале 2023 года: [Электронный ресурс]. URL: https://spbit.ru/news/Statistika-DDoS-atak-v-pervom-kvartale-2023-goda-272089. (Дата обращения: 30.10.2023).