ДОПОЛНЕНИЕ МЕТОДА МОДЕЛИРОВАНИЯ УГРОЗ, ОСНОВАННОГО НА ШАБЛОНЕ

В. А. Макаревич

Белорусский государственный университет, г. Минск;
ulad.makarevich@gmail.com;
науч. рук. – Е. А. Минюкович, канд. экон. наук, доц.

Статья посвящена возрастанию количества, многообразия и стоимости атак на корпоративные информационные системы и роли персонала организации в их предотвращении. Обоснована разработка метода моделирования угроз, основанного на шаблоне. Обсуждается проведенная работа по совершенствованию метода. Предложено внедрение способов агрегации и визуализации результатов в шаблон моделирования угроз для обеспечения возможности использования в качестве основы будущих моделей, практик и сценариев стратегического управления информационной безопасностью.

***Ключевые слова*:** информационная безопасность; управление информационной безопасностью; анализ угроз; моделирование угроз; шаблон моделирования угроз.

Ключевое место в бизнес-процессах организаций – начиная с организации производства и предоставления услуг и заканчивая обеспечением коммуникаций внутри команды и с клиентами – сегодня занимает сбор всевозможных данных и информации, в том числе о клиентах. Взаимодействие с большими объемами данных позволяет повысить эффективность работы и извлечь новые идеи для лучшего понимания своей операционной деятельности, принятия управленческих решений и изучения своих клиентов. В то же время большие объемы данных подвергают организации и их клиентов потенциальным рискам. Вместе с внедрением информационных технологий растет количество, многообразие и стоимость атак на корпоративные информационные системы организаций, которые становятся все более уязвимыми. Несмотря на создание более совершенных и безопасных систем ИТ-специалистами, число инцидентов информационной безопасности не уменьшается.

Управление рисками кибербезопасности исторически относилось к компетенции технических специалистов и экспертов. Однако данную задачу больше нельзя делегировать исключительно команде ИТ-специалистов вне зависимости от ее размера. Напротив, руководящий состав во всех сферах экономики и государственного управления должен осознавать, каким образом информационная безопасность соотносится с их ролями и обязанностями, и обратить внимание на ее динамичный и быстроразвивающийся ландшафт, состоящий из непредсказуемых, сложных и по-новому выстроенных киберугроз.

Разработка мер и решений по обеспечению безопасности корпоративных информационных систем требует иного мышления, которое будет рассматривать кибербезопасность не как конечную проблему, которую можно решить один раз, но как непрерывный процесс. Следовательно, ее менеджмент должен быть направлен не на снижение вероятности возникновения рисков, а на их управление.

В процессе исследований мы разработали метод моделирования угроз, основанном на шаблоне, целью которого является обеспечение помощи в принятии управленческих решений на основе своевременного моделирования угроз. Метод моделирования угроз основан на шаблоне, состоящем из восьми базовых элементов процесса моделирования, поэтапное рассмотрение которых позволяет оценить информационную безопасность корпоративной информационной системы и ландшафт потенциальных угроз, разработать решения по управлению потенциальными угрозами [1].

Метод отталкивается от положения, что суждения о кибербезопасности часто оказываются предвзятыми и неполными в предсказуемо проблематичных направлениях, что вызывает проблемы при принятии решений о необходимости инвестиций и их распределении при ее обеспечении в организации. Использование метода вовлекает всех сотрудников организации, включая руководителей, ИТ-специалистов и менеджеров, занимающих различные должности, в процесс моделирования, что помогает обеспечить грамотное распределение инвестиций и принятие управленческих решений в области информационной безопасности, учесть человеческий фактор и роли сотрудников, выработать необходимые коммуникации и методы реагирования на инциденты [2].

После апробации, проведенной в ОАО «Белорусская универсальная товарная биржа», мы получили обратную связь о преимуществах и проблемных местах метода [3]. Основываясь на предложениях, мы провели работу по следующим направлениям:

- Уточнение и разработка блоков шаблона, связанных с анализом злоумышленников и угроз. Так, были внесены изменения в исходный шаблон, уточняющие понятия целей злоумышленников и возможных уязвимостей, что позволяет участникам процесса определить и характеризовать направления возможных атак благодаря выявлению, отслеживанию и поддержке перечня уязвимостей активов организации. Также в шаблон был добавлен блок анализа опыта и текущих возможностей организации по противодействию угрозам, выявленным ранее, что позволяет дать оценку текущему состоянию защиты системы.

• Доработка связей шаблона с существующими стандартами, политиками и практиками в области информационной безопасности. Была предусмотрена возможность проведения анализа текущей ситуации и разработки мер совершенствования системы информационной безопасности при согласовании с существующими актами и фреймворками. Данное решение позволит руководящему составу разработать стратегию кибербезопасности вне зависимости от размера и направления деятельности организации.

На данный момент мы проводим анализ возможности внедрения существующих способов агрегации и визуализации результатов моделирования, что позволит организациям использовать результаты процесса моделирования в качестве основы будущих моделей, практик и сценариев стратегического управления информационной безопасностью. В частности, для обеспечения возможности обеспечения принятия управленческих решений, ведется разработка представления ключевых тезисов об уровнях защиты организации, способах обнаружения инцидентов, планах реагирования, а также распределении обязанностей и ролей в случае их возникновения.

Библиографические ссылки

1. *Макаревич, В. А., Минюкович, Е. А., Мулярчик, К. С.* Анализ и моделирование угроз информационной̆ безопасности предприятия на основе универсального шаблона // Журнал Белорусского государственного университета. Экономика. 2021. №1. С. 57–68.
2. *Parenty, T. J.* A Leader's Guide to Cybersecurity: Why Boards Need to Lead – and How to Do It. Boston, 2019. 240 p.
3. *Макаревич, В. А., Макаревич, В. А., Минюкович, Е. А.* Апробация метода моделирования угроз, основанного на шаблоне // Актуальные проблемы науки XXI века. 2021. №10. С. 16–20.