УДК 330.47

РАССМОТРЕНИЕ ВОПРОСОВ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ПРОВЕДЕНИИ МЕРОПРИЯТИЙ ПО МОДЕЛИРОВАНИЮ УГРОЗ

В. А. Макаревич

старший преподаватель, Белорусский государственный университет, экономический факультет, г. Минск, Республика Беларусь, e-mail: ulad.makarevich@gmail.com

Автор проводит анализ вопросов конфиденциальности, которые возникают при проведении мероприятий по моделированию угроз. Рассматриваются возможные решения для их устранения, среди которых авторы выделяют привлечение экспертов в области конфиденциальности, разработку четких требований к обеспечению конфиденциальности и соответствующих инструментов моделирования, и включение оценки воздействия на конфиденциальность в процесс моделирования.

Ключевые слова: конфиденциальность; моделирование угроз; требования к конфиденциальности; инструменты моделирования угроз; оценка воздействия на конфиденциальность.

ADDRESSING PRIVACY CONCERNS WHEN CONDUCTING THREAT MODELING ACTIVITIES

U. A. Makarevich

senior lecturer, Belarusian State University, faculty of economics, Minsk, Republic of Belarus, e-mail: ulad.makarevich@gmail.com

The author analyzes privacy concerns that arise when conducting threat modeling activities. Possible solutions to address them are considered, among which the authors highlight the engagement of privacy experts, development of clear privacy requirements and appropriate modeling tools, and incorporation of privacy impact assessment into the modeling process.

Keywords: privacy; threat modeling; privacy requirements; threat modeling tools; privacy impact assessment.

Конфиденциальность является важным аспектом безопасности, которому в последние годы уделено значительное внимание. Цифровая экономика выходит за рамки исключительно электронной коммерции и затрагивает инфраструктуру и устройства, которые мы используем для доступа к глобальной сети. Вместе с этим увеличивается объем собираемых и обрабатываемых данных о пользователях и клиентах. Это актуализирует необходимость обеспечения рассмотрения фактора конфиденциальности при разработке информационных систем и продуктов организаций и предприятий. Моделирование угроз представляет собой подход, используемый для выявления и снижения рисков безопасности при разработке системы информационной безопасности организации и ее продуктов. Однако большая часть методов моделирования угроз не учитывает влияние конфиденциальности, тем самым подвергая риску данные сотрудников и клиентов. По этой причине крайне важно рассмотреть вызовы, возникающие в области конфиденциальности при моделировании угроз, и предложить возможные решения для их предотвращения.

Данная работа основана на тщательном обзоре литературы, включая научные статьи, материалы конференций и доклады по теме конфиденциальности и моделированию угроз. Анализ был направлен на изучение проблем, связанных с обеспечением конфиденциальности при моделировании угроз, и решений, предложенных для снижения влияния данных проблем. Литературный обзор был проведен с соблюдением строгих критериев поиска, благодаря которым в анализ были включены наиболее актуальные публикации.

В ходе анализа был выявлен ряд проблем, касающихся конфиденциальности и возникающих при моделировании угроз. Одной из существенных проблем является недостаток экспертизы в области конфиденциальности среди специалистов по вопросам информационной безопасности. За прошедшее время было разработано множество подходов и методологий моделирования угроз, которые варьируются от теоретических концепций до практических [1; 2]. Однако большинство методов моделирования угроз не учитывают аспект конфиденциальности. Прежде всего это можно объяснить нехваткой экспертов в области конфиденциальности, помощь которых необходима для выявления и снижения рисков нарушения конфиденциальности при разработке информационных систем. Поэтому необходимо привлекать подобных экспертов для участия в процессах моделирования угроз, чтобы обеспечить должное рассмотрение вопросов конфиденциальности.

Еще одной проблемой, возникающей при моделировании угроз, является отсутствие четких требований к обеспечению конфиденциальности. Зачастую такие требования носят размытый и неоднозначный характер, что затрудняет выявление рисков конфиденциальности и разработку соответствующих стратегий по их снижению. Поэтому для обеспечения защиты организации и ее клиентов необходимо иметь четкие и хорошо сформулированные требования к обеспечению конфиденциальности, которые бы описывали конкретные потребности системы или программного обеспечения в поддержке конфиденциальности. Данные требования должны охватывать все аспекты конфиденциальности, включая сбор, хранение, обмен и удаление данных, и должны быть разработаны с учетом юридических и этических обязанностей организации. Разработка четких и хорошо сформулированных требований к обеспечению конфиденциальности предполагает совместные усилия различных заинтересованных сторон внутри организации, а также регулярное обновление с учетом изменений в операционной среде.

Отсутствие соответствующих инструментов моделирования угроз также представляет собой серьезную проблему. Как отмечают исследователи, моделирование угроз в настоящее время находится на очень низком уровне зрелости с точки зрения исследований, поддержки инструментов, и практической разработки [3]. Так, несмотря на наличие описания подходов к моделированию и отчетов об опыте применения и исследований, демонстрирующих широкую применимость в различных областях, они не включают в себя информацию о лучших практиках и барьерах при внедрении, что мешает разработать инструменты, специфические для конкретной области. Следовательно, дальнейшая разработка методов моделирования угроз и соответствующих инструментов для обеспечения комплексной защиты конфиденциальности позволит организациям создавать безопасные и надежные системы, защищающие личную информацию сотрудников и клиентов от несанкционированного доступа и неправомерного использования.

В дополнение к перечисленному, моделирование угроз часто не включает в себя оценку воздействия на конфиденциальность. Оценка воздействия на конфиденциальность обеспечивает структурированный подход к определению и оценке потенциальных рисков в области конфиденциальности, связанных с разрабатываемой системой. Данный подход включает анализ процессов организации с целью выявления того, как они влияют или могут повлиять на конфиденциальность лиц, чьи данные она хранит, собирает или обрабатывает. Следовательно, без подобного мероприятия, участники процесса моделирования угроз не смогут выявить потенциальные угрозы конфиденциальности и разработать стратегии по их предотвращению или подавления.

Таким образом, в результате проведенного анализа выявлено, что существует ряд вопросов конфиденциальности при проведении мероприятий по моделированию угроз. Данные вопросы обусловленных, главным образом, недостатком опыта в области конфиденциальности, неоднозначностью требований, отсутствием соответствующих инструментов моделирования угроз и оценки воздействия на конфиденциальность. Устранение данных проблем позволит организациям повысить эффективность выявления и снижения рисков в области конфиденциальности данных сотрудников и клиентов, а также обеспечит их инструментами для разработки актуальных стратегий по устранению и предотвращению соответствующих угроз.

Библиографические ссылки

1. *Макаревич В. А., Минюкович Е. А., Мулярчик К. С.* Анализ и моделирование угроз информационной безопасности предприятия на основе универсального шаблона // Журнал Белорусского государственного университета. Экономика / Белорус. гос. ун-т. 2021. Вып. 1. С. 57–68.

2. *Tuma K., Calikli G., Scandariato R.* Threat analysis of software systems: A systematic literature review // Journal of Systems and Software. Elsevier. 2018. Vol. 144. P. 275–294.

3. *Yskout K., Heyman T., Landuyt D., Sion L., Wuyts K., Joosen W.* Threat modeling: from infancy to maturity // Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER '20) / Association for Computing Machinery. 2020. P. 9–12.