УДК 330.47

РАЗВИТИЕ ЧЕЛОВЕКО-ОРИЕНТИРОВАННОГО ПОДХОДА К МОДЕЛИРОВАНИЮ УГРОЗ

В. А. Макаревич[1)], В. А. Макаревич[2)], Е. А. Минюкович[3)]

[1)] *аспирант, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: ulad.makarevich@gmail.com*

[2)] *аспирант, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: makarevich.vaa@gmail.com*

[3)] *кандидат экономических наук, доцент, кафедра цифровой экономики, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: miniukovich@bsu.by*

Обосновывается разработка метода моделирования угроз, основанного на шаблоне. Характеризуется роль человека в инцидентах информационной безопасности. Обсуждается направление разработки предложенного метода моделирования угроз с учетом человеко-ориентированного подхода и существующих практик, и методологий.

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

DEVELOPMENT OF A HUMAN-CENTERED APPROACH TO THREAT MODELING

U. A. Makarevich[1)], V. A. Makarevich[2)], K. A. Miniukovich[3)]

[1)] *Postgraduate Student, Belarusian State University, Minsk, Republic of Belarus, e-mail: ulad.makarevich@gmail.com*

[2)] *Postgraduate Student, Belarusian State University, Minsk, Republic of Belarus, e-mail: makarevich.vaa@gmail.com*

[3)] *PhD in Economics, Associate Professor, Department of Digital Economy, Belarusian State University, Minsk, Republic of Belarus, e-mail: miniukovich@bsu.by*

The development of a template-based threat modeling method is justified. The role of the human in cybersecurity incidents is highlighted. The direction of development of the proposed threat modeling method, based on the human-centered approach and existing practices and methodologies, is discussed.

Keywords: information security; information security management; threat analysis; threat modeling; threat modelling canvas.

Задача обеспечения информационной безопасности организации является одним из ключевых аспектов корпоративных ИТ-систем. За последние годы риски информационной безопасности стали более распространенными, а пандемия COVID-19 только усугубила ситуацию: ускорившиеся темпы внедрения информационных технологий в бизнес-процессы организаций и повсеместное использование облачных вычислений как основного вектора развития корпоративных информационных технологий увеличивают площадь покрытия потенциальных атак.

Бизнес-процессы во многом зависят от надежного и непрерывного функционирования критической инфраструктуры, повышенная сложность и взаимосвязанность систем которой являются объектами современных киберугроз. Подобно репутационным, финансовым и прочим, риски информационной безопасности прямым образом оказывают влияние на прибыль компании. Увеличение количества и разнообразия инцидентов информационной безопасности способствует увеличению расходов и прямым образом влияет на доходы. Так, вывод из строя ключевых элементов информационной инфраструктуры может лишить организацию возможности внедрять инновации в операционную и проектную деятельность, а также привлекать и удерживать клиентов.

Информационная безопасность является важным элементом общего управления рисками организации. Следствием этого являются рост инвестиций в кибербезопасность и разработка стратегий, направленных на устранение слабых мест системы, которыми могут попытаться воспользоваться злоумышленники. Хотя эти подходы могут предотвратить проникновение злоумышленника извне, они не всегда направлены на устранение основных факторов, создающих уязвимости.

Одним из подходов для упреждающего решения проблем информационной безопасности корпоративных систем является моделирование угроз, которое включает в себя идентификацию ключевых активов системы и угроз данным активам [1]. Процесс моделирования используется как для оценки текущего состояния системы, так и в качестве инструмента обеспечения безопасности при разработке новых систем. На основе проводимого анализа, результатом которого являются объективные оценки состояния системы информационной безопасности и ландшафта потенциальных угроз, возможно разработать средства управления для предотвращения и противодействия потенциальным угрозам.

В ходе проведенных исследований мы разработали метод моделирования угроз, основанный на шаблоне, который помогает своевременно прорабатывать текущие угрозы и принимать эффективные управленческие решения в рамках руководства информационной безопасностью организации. Метод позволяет принимать во внимание действия пользователей внутри системы благодаря привлечению основных элементов организаций – членов руководящего состава, специалистов по кибербезопасности,

ИТ-отдела, производственного персонала, и профильных специалистов – к процессу моделирования.

Данное направление разработки обосновано тем, что вне зависимости от создания более совершенных и безопасных систем ИТ-специалистами, остается риск, от которого данные системы не способны избавиться – люди. В то время как обход и компрометация каждой новой технологии злоумышленниками представляет собой лишь вопрос времени, значительную роль в инцидентах информационной безопасности играют индивидуальные поведенческие ошибки. Злоумышленники используют факт того, что люди склонны доверять определенным запросам, переходить по ссылкам и открывать зараженные вирусами прикрепленные вложения. Так, согласно отчету Proofpoint, значительно возросло количество атак, предполагающих взаимодействие с прикрепленными вложениями, в отдельных случаях достигая 10-кратного увеличения [2].

Таким образом, метод моделирования угроз, основанный на шаблоне, позволяет обеспечить новый, ориентированный на взаимодействие людей, подход к управлению информационной безопасностью организации. Руководители не могут отказываться от надзора за кибербезопасностью или делегировать его операционным менеджерам, полагаясь на отдел безопасности, когда речь идет о защите информации организации, инвестиционных решениях о внедрении решений по ее обеспечению. Для создания осознанной культуры безопасности необходимо организовать возможность каждого члена команды принимать участие в анализе и разработке системы информационной безопасности, тем самым выходя за рамки стандартных одно-двухдневных тренингов, принятых во многих компаниях, и перенимая определенные мыслительные и поведенческие паттерны.

Для определения направлений дальнейшей практической разработки метода мы провели апробацию в ОАО «Белорусская универсальная товарная биржа», в ходе которой были выявлены его преимущества и проблемные места [3]. На данный момент проводится доработка модели для обеспечения применения метода моделирования угроз в качестве базиса при принятии управленческих решений.

В первую очередь мы рассматриваем существующие политики, стандарты и практики обеспечения информационной безопасности. Поскольку составление плана противодействия не входит в обязанности руководителя, необходимо проанализировать, систематизировать и обеспечить согласование с существующими актами и фреймворками, которые могут помочь организациям любого масштаба в разработке стратегии кибербезопасности. Одним из примеров подобных документов является NIST Cybersecurity Framework, разработанный Национальным институтом стандартов и технологий США (NIST) [4]. Данный фреймворк прост в использовании и предоставляет руководителям и директорам эффективную структуру для обсуждения важных аспектов информационной безопасности организации. В то же время он содержит множество уровней детализации, которые специали-

сты в сфере ИТ и кибербезопасности могут использовать для разработки средств контроля, процессов и процедур.

Стоит отметить, что доработка осуществляется с учетом первоначальной ориентации метода моделирования угроз, основанного на шаблоне, на человека. Понятия и определения, используемые для управления организацией и управления информационной безопасностью, отличаются: руководящий состав и производственный персонал организации могут быть не полностью осведомлены о техническом, организационном и операционном уровнях обеспечения кибербезопасности. Поэтому для выполнения требований контроля необходимы адекватные политики и процедуры, которые устанавливались бы руководством и позволяли бы каждому сотруднику организации обеспечивать необходимый уровень защиты.

Ориентация на достижение общих целей, таких как обеспечение безопасности организации, непрерывности бизнес-процессов и сокращение репутационных рисков позволяет сократить разрыв между ролями специалистов по информационной безопасности и других элементов организации. Поэтому задача доработки метода моделирования угроз, основанного на шаблоне, заключается в обеспечении установления четкой и последовательной коммуникации для обмена полезными и объективными метриками взаимодействия с информацией, обеспечения системного контроля и анализа поведения людей и сравнение с лучшими практиками и методологиями управления рисками.

Библиографические ссылки

1. UcedaVelez T., Morana M. M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Hoboken : John Wiley & Sons, 2015. 696 p.

2. The Human Factor 2021: Cybersecurity, Ransomware and Email Fraud in a Year that Changed the World / Proofpoint : site. URL: https://www.proofpoint.com/sites/default/-files/threat-reports/pfpt-us-tr-human-factor-report.pdf (date of access: 29.04.2022).

3. Макаревич В. А., Макаревич В. А., Минюкович Е. А. Апробация метода моделирования угроз, основанного на шаблоне // Актуальные проблемы науки XXI века : сб. науч. ст. молодых ученых / Минский инновационный ун-т. Минск, 2021. Вып. 10. С. 16–20.

4. Framework for Improving Critical Infrastructure Cybersecurity / National Institute of Standards and Technology site. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/-NIST.CSWP.04162018.pdf (date of access: 29.04.2022).