РАЗРАБОТКА МЕТОДА МОДЕЛИРОВАНИЯ УГРОЗ НА ОСНОВЕ ШАБЛОНА ДЛЯ АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

В. А. Макаревич, В. А. Макаревич

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

Статья посвящена возрастанию темпов цифровой трансформации экономики и его влиянию на информационную безопасность организаций. Подчеркивается необходимость моделирования угроз как необходимого элемента процесса совершенствования и разработки информационных систем. Обоснована необходимость разработки универсального метода моделирования угроз. Предложен метод моделирования угроз, основанный на шаблоне. Подчеркивается возможность использования разработанного метода в процессе обучения сотрудников основам информационной и цифровой безопасности.

Ключевые слова: информационная безопасность; моделирование угроз; шаблон моделирования угроз.

В условиях цифровой трансформации безопасность данных и информации является одним из основных условий жизнеспособности организации. Несмотря на то, что до середины 2020 г. цифровая трансформация экономики была скорее распространенной темой для обсуждения, чем фактором влияния на дальнейшие действия, пандемия COVID-19 изменила взгляды бизнес-сообщества, ускорив в пять раз смещение методик и инструментария в сторону цифровизации и переосмысления бизнес-процессов [1]. Благодаря внедрению информационных технологий в бизнес-процессы, организациям удалось сократить личные контакты, тем самым сохранив здоровье и благополучие своих сотрудников и клиентов. Однако подобные изменения стали катализатором увеличившегося количества атак на системы информационной безопасности организаций.

В связи с постоянным увеличением разнообразия способов атак организациям необходимо совершенствоваться и разрабатывать новые и лучшие методы защиты своих информационных систем. Подобная деятельность невозможна без полноценного рассмотрения ландшафта угроз, т.е. событий, которые могут нарушить конфиденциальность, целостность или доступность информационных систем в результате несанкционированного доступа, неправильного использования, изменения и уничтожения информации или информационной системы. Решением данной проблемы является моделирование угроз — процесс применения стратегического

подхода, основанного на рисках, к систематическому выявлению и устранению угроз системы [2]. Данный процесс помогает изучить потенциальные угрозы информационных и бизнес-систем и выработать соответственные меры по их предупреждению или устранению.

Для обеспечения целостного подхода к моделированию необходимо осознавать все возможные и текущие угрозы информационной безопасности, которые существуют на каждом уровне взаимодействия организации с ее внутренней и внешней средой. Таким образом, организация не должна рассматривать кибербезопасность в качестве зоны ответственности исключительно ИТ-отдела, но должна относиться к ней как к результату взаимодействия каждого ее элемента: руководства, специалистов по кибербезопасности, ИТ-отдела, производственного персонала, и профильных специалистов [3].

В ходе исследования мы пришли к выводу, что существующие методы моделирования угроз содержат ограничения. Во-первых, они обычно рассматривают не все необходимые компоненты моделирования, но детально прорабатывают один или несколько элементов конкретной направленности. Во-вторых, существующие методы сложны, что ограничивает возможность их использования сотрудниками, которые не обладают знаниями и навыками в сфере информационной и цифровой безопасности. Это в свою очередь приводит к невозможности применения целостного подхода, отмеченного выше, и, как следствие, к упущению возможных угроз и разработке неполных и неактуальных ответных и предупредительных мер.

Следовательно, необходимо разработать инструмент, который должен быть доступным для сотрудников с разным уровнем подготовки в сфере информационной и цифровой безопасности и может обеспечить элементы организации всеми необходимыми навыками моделирования угроз.

В результате исследования мы разработали метод моделирования угроз, основанный на шаблоне, который может устранить выявленные недостатки и позволяет быстро и продуктивно провести процесс моделирования (рис. 1). Шаблон включает в себя все ключевые элементы моделирования угроз и содержит в своей основе структурный подход к моделированию. Особенное отличие метода – его доступность для людей с разной подготовкой в сфере информационной безопасности.

Шаблон был апробирован на занятиях со студентами экономического факультета Белорусского государственного университета в рамках дисциплин «Цифровая безопасность», «Информационная безопасность», «Бизнес-офис организации (предприятия) и интернет-маркетинг». Наблюдение за взаимодействием студентов с шаблоном и последующий

сбор обратной связи позволили внести изменения в его структуру и логику с целью увеличения доступности:

- шаблон разбивает страницу на четыре основных компонента, которые характеризуют активы, злоумышленников, угрозы и анализ рисков и разделяются на составляющие их элементы для последовательного заполнения;
- структура шаблона адекватно декомпозирована, чтобы не отвлекать от основной цели моделирования;
- благодаря простому визуальному и текстовому изложению, шаблон позволяет пользователю понять структуру и порядок заполнения шаблона и сразу приступить к процессу моделирования.

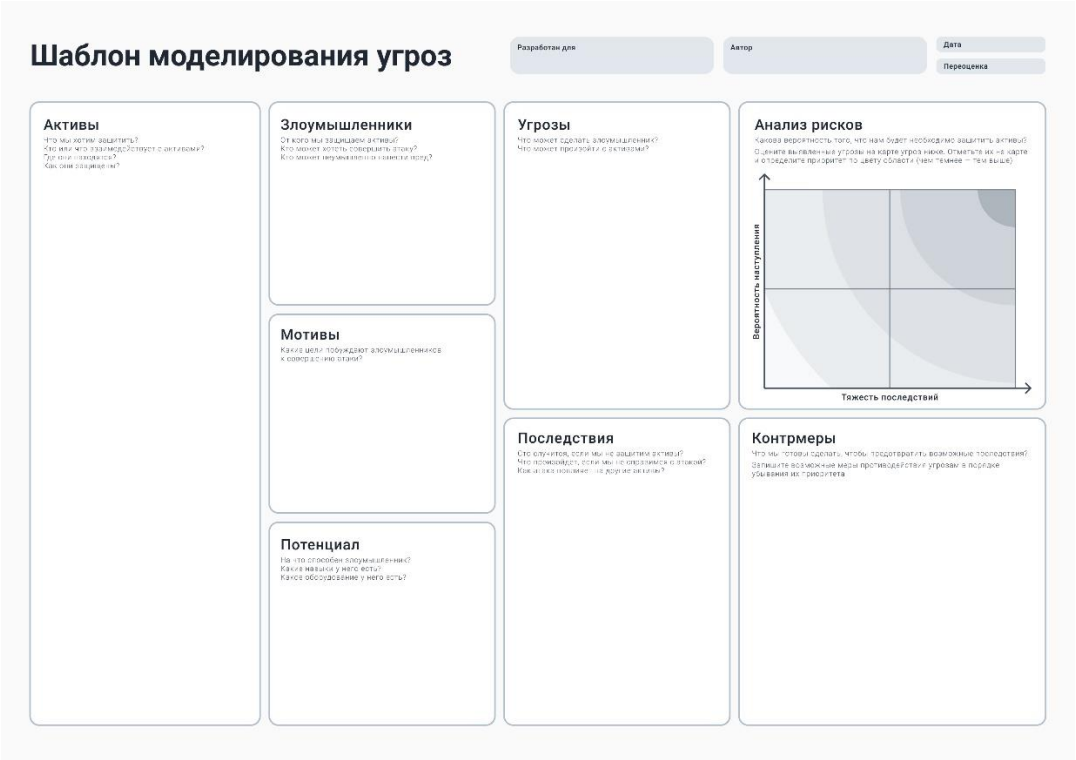

Рис. 1. – Шаблон моделирования угроз.

Одним из возможных вариантов применения метода также является его использование при обучении персонала с целью получения сотрудниками организации необходимых навыков для анализа угроз и связанных с ними рисков, а также для осознания своей роли в обеспечении целостной системы информационной безопасности организации.

На данный момент мы апробируем практическое применение предложенного нами метода моделирования угроз на основе шаблона в организации для анализа потенциальных угроз информационных и бизнес-систем с целью совершенствования метода на основе получения обратной связи от организаций.

Библиографические ссылки

1. Meet the 2020 consumers driving change // IBM Institute for Business Value [Electronic resource]. URL: https://www.ibm.com/thought-leadership/institute-business-value/report/consumer-2020# (date of access: 04.04.2021).
2. UcedaVelez T., Morana M. M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Hoboken: John Wiley & Sons, 2015.
3. Макаревич, В. А., Минюкович, Е. А., Мулярчик, К. С. Проблемы информационной безопасности при организации удаленной работы сотрудников // Актуальные проблемы науки XXI века. 2020. №1(9). С. 12-16. с.