УДК 330.47

М. Деловое администрирование и экономика бизнеса. Маркетинг. Бухучет. Экономика персонала
M. Business Administration and Business Economics; Marketing; Accounting; Personnel Economics

АНАЛИЗ И МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА ОСНОВЕ УНИВЕРСАЛЬНОГО ШАБЛОНА

***В. А. МАКАРЕВИЧ*[1)], *Е. А. МИНЮКОВИЧ*[1)], *К. С. МУЛЯРЧИК*[1)]**

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Отмечается, что безопасность данных и информации является ключевым условием жизнеспособности организации и в условиях цифровизации экономики субъектам хозяйствования необходимо повышать эффективность защиты своих информационных систем. Указывается, что моделирование угроз помогает организациям осознать потенциальные риски для информационных и бизнес-систем, а также разработать конкретные меры по их предупреждению или устранению. Рассматриваются основные компоненты моделирования угроз, анализируются наиболее часто используемые методы моделирования, указываются их недостатки. Предложен авторский метод устранения выявленных недостатков, основанный на шаблоне моделирования угроз. Разработан и апробирован подход к обучению применению данного метода.

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

ORGANISATION'S INFORMATION SECURITY THREAT ANALYSIS AND MODELLING BASED ON A UNIVERSAL CANVAS

***U. A. MAKAREVICH*[a], *K. A. MINIUKOVICH*[a], *K. S. MULYARCHIK*[a]**

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*
Corresponding author: U. A. Makarevich (ulad.makarevich@gmail.com)

Образец цитирования:
Макаревич ВА, Минюкович ЕА, Мулярчик КС. Анализ и моделирование угроз информационной безопасности предприятия на основе универсального шаблона. *Журнал Белорусского государственного университета. Экономика*. 2021;1:57–68.

For citation:
Makarevich UA, Miniukovich KA, Mulyarchik KS. Organisation's information security threat analysis and modelling based on a universal canvas. *Journal of the Belarusian State University. Economics.* 2021;1:57–68. Russian.

Авторы:
Влад Александрович Макаревич – старший преподаватель кафедры цифровой экономики экономического факультета.
Екатерина Александровна Минюкович – кандидат экономических наук, доцент; доцент кафедры цифровой экономики экономического факультета.
Константин Сергеевич Мулярчик – кандидат технических наук, доцент; доцент кафедры телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий.

Authors:
Ulad A. Makarevich, senior lecturer at the department of digital economics, faculty of economics.
k.mulyarchik@gmail.com
https://orcid.org/0000-0001-9926-2614
Katsiaryna A. Miniukovich, PhD (economics), docent; associate professor at the department of digital economics, faculty of economics.
miniukovich@bsu.by
https://orcid.org/0000-0002-9782-5468
Konstantin S. Mulyarchik, PhD (engineering), docent; associate professor at the department of telecommunications and information technologies, faculty of radiophysics and computer technologies.
ulad.makarevich@gmail.com
https://orcid.org/0000-0001-6255-1471

Security of data and information is key to the viability of an organisation. With the digitalisation of the economy, business entities need to evolve towards more effective protection of their information systems. Threat modelling helps organisations understand potential threats to information and business systems, and develop specific measures to prevent or eliminate threats. The authors review the main components of threat modelling as well as analyse and identify the shortcomings of the most commonly used modelling methods. The article proposes the author's method based on the threat modelling canvas, that allows to eliminate the identified shortcomings. The authors have also developed and approbated an approach to teaching the use of this method.

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

Введение

Ускорение цифровизации экономики, вызванное переходом на удаленную работу в связи с пандемией COVID-19, стало катализатором количества атак на системы информационной безопасности организаций на прикладном уровне и в облаке. Безопасность данных сегодня является ключевым условием жизнеспособности организации. В условиях растущего многообразия способов атак необходимо искать лучшие методы защиты. Однако разработка защищенных систем и их компонентов невозможна без осознания ландшафта угроз – событий, которые могут нарушить конфиденциальность, целостность или доступность информационных систем в результате несанкционированного доступа, неправильного использования, изменения и уничтожения информации. Моделирование угроз помогает организациям установить потенциальные угрозы для своих информационных и бизнес-систем и принять конкретные меры по их предупреждению или устранению.

Организации должны применять более целостный подход к обеспечению информационной безопасности, что возможно только при взаимодействии всех элементов бизнес-системы: руководства организации, специалистов по кибербезопасности, ИТ-отдела, производственного персонала и профильных сотрудников [1; 2]. В то же время эффективную систему нельзя построить без осознания возможных и текущих угроз, которые присутствуют на каждом уровне взаимодействия организации с внутренней и окружающей средой.

Таким образом, необходимо найти доступный для людей с разным уровнем подготовки в сфере информационной и цифровой безопасности инструмент, который обеспечит все элементы организации необходимыми навыками моделирования угроз и связанных с ними рисков. Это позволит развить осведомленность и культуру команды в области защиты данных и информации и поможет осознать личную ответственность каждого сотрудника за безопасность организации.

В данной работе мы рассматриваем основные компоненты и категории моделирования угроз, анализируем особенности и недостатки широко используемых методов каждой из категорий, обосновываем необходимость разработки универсального метода моделирования угроз, учитывающего выявленные недостатки и доступного для сотрудников с разным уровнем подготовки в области информационной и цифровой безопасности. Представлен метод моделирования угроз, разработанный на основе шаблона моделирования угроз. Структура последнего опирается на метод, предложенный Фондом электронных рубежей[1]. Указанный метод апробирован в ходе занятий со студентами экономического факультета БГУ. Исходя из опыта взаимодействия и обратной связи, также разработан подход к обучению данному методу.

Основные компоненты моделирования угроз

Моделирование угроз – это процесс использования стратегического подхода, основанного на рисках, к систематическому выявлению и устранению угроз [3]. Данный процесс является проактивным, предполагает определение критических областей проектирования, разработку процедур для их установления и применение соответствующих контрмер. Моделирование позволяет приоритизировать угрозы в целях достижения эффективного распределения ресурсов и уделяемого им внимания, основываясь на рисках, воздействии на деятельность организации и стоимости мер реагирования.

Широкий спектр применения моделирования угроз, включая разработку и функционирование программного обеспечения (ПО), приложений, систем, бизнес-процессов и т. д., делает его универсальным инструментом принятия обоснованных решений по защите компонентов различных сфер деятельности организаций. Процесс моделирования может быть инициирован на любой стадии проекта в целях максимальной эффективности разработанных решений по противодействию угрозам.

[1]Electronic frontier foundation. Threat modelling [Electronic resource]. URL: https://sec.eff.org/topics/threat-modeling (date of access: 25.01.2021) ; Electronic frontier foundation. Your security plan [Electronic resource]. URL: https://ssd.eff.org/en/module/your-security-plan (date of access: 25.01.2021).

Мы выделяем две стадии, в ходе которых моделирование наиболее желательно: раннюю стадию разработки – для использования полученных результатов в последующем проектировании, стадию эксплуатации и функционирования – для переоценки угроз в целях обеспечения соответствия мер защиты изменяющимся угрозам.

На основе сведений из [3–5] в моделировании угроз можно выделить шесть основных компонентов: анализ угроз, идентификацию активов, определение векторов атак, оценку потенциала смягчения последствий, оценку рисков и составление карты угроз (картирование). Необходимо в полной мере учитывать каждый, поскольку отсутствие одного или нескольких приведет к неполноте модели и ненадлежащему устранению или предотвращению возможных угроз.

Анализ угроз часто осуществляется специалистами по информационной безопасности. Источниками анализа являются открытые и закрытые базы данных, существующие решения и сервисы для обеспечения безопасности информационных систем. Сведения о типах и видах угроз, мотивах злоумышленников, инструментах и методах, используемых ими при компрометации информации и взломе информационных систем, механизмах их обнаружения и кейсах организаций структурируются, анализируются и используются в целях расширения понятийного, теоретического и методологического аппарата специалистов информационной безопасности и разработки аргументированных контрмер.

Идентификация активов подразумевает определение данных, информации, сервисов, необходимых или критически важных для полноценного функционирования системы. Дополнением к идентификации является инвентаризация компонентов, содержащих указанные активы. Инвентаризация включает обзор способов хранения, обработки и взаимодействия активов с системой организации, а также перечня используемых мер безопасности по отношению к ним. Такое дополнение позволяет специалистам в режиме реального времени отслеживать изменения и уязвимости в существующих активах.

Определение векторов атак необходимо для принятия решений по устранению угроз активам организации. Данный этап заключается в выявлении, отслеживании уязвимостей всех компонентов проведенной ранее инвентаризации. После сбора и анализа информации следует рассмотреть возможные подходы злоумышленников к атакам на системы организации, принимая во внимание их вероятные цели, мотивы и возможности, чтобы определить потенциальные способы компрометации активов.

Оценка потенциала смягчения последствий включает анализ как опыта и способностей организации в области информационной безопасности, так и применяемых ей методов обнаружения, реагирования и защиты от конкретных видов угроз. Он позволяет установить текущий уровень защиты системы и принять решение о вложении дополнительных средств для сокращения угрозы и ее последствий.

Оценка рисков обеспечивает понимание текущего состояния системы информационной безопасности в целях разработки, внедрения, обновления и применения соответствующих мер противодействия угрозам. В рамках оценки рисков происходит анализ соотношения текущих и возможных угроз и имеющихся активов, также может проводиться активное тестирование систем и мер защиты на уязвимость, например тестирование на проникновение [6]. В результате специалисты приоритизируют угрозы, определяют среди них имеющие наибольший уровень риска и смягчают их с применением соответствующих контрмер.

Составление карты (картирование) угроз нацелено на анализ подверженности риску смежных активов. На данном этапе необходимо рассмотреть возможные способы перемещения злоумышленников между активами и последствия применения мер по снижению риска для всей системы. Картирование позволяет предвидеть эффективность контрмер и инициировать их развитие в многоуровневые или прикладные структуры, позволяющие снизить воздействие угроз.

Влияние угроз на деятельность организации является отдельным фактором моделирования. Риски информационной безопасности влияют на три ее основных элемента: конфиденциальность, целостность и доступность данных. Необходимо оценивать экономический эффект от компрометации или утери актива организации. Для этого следует учитывать экономический контекст системы, совместив анализ активов с их функциями в бизнес-процессах.

Анализ методов моделирования угроз

Сегодня разработаны большое количество методов моделирования угроз, которые можно классифицировать различными способами в зависимости от направленности. Не все методы многофункциональны и способны к расширению. Так, например, одни из них достаточно абстрактные, а другие ориентированы исключительно на риск или защиту частной жизни и информации. Выбор в пользу того или иного метода стоит делать с учетом рассматриваемой системы и имеющихся инструментов. Также отметим, что для обеспечения всестороннего рассмотрения конкретной проблемы методы могут дополнять друг друга.

Обобщая сведения из источников [3; 4; 7], можно условно разделить методы моделирования угроз на три основные категории: системно ориентированные, ориентированные на ресурсы и ориентированные на атаку.

Целью *системно ориентированных методов* является обеспечение полного понимания системы, для которой будет создаваться модель угроз. До процесса моделирования происходят разработка и тщательная проверка системы. Данные методы обычно используются для моделирования угроз сетей и комплексных систем, в том числе ПО. В качестве иллюстрации метода выступают компонентные диаграммы, а также диаграммы потока данных (*DFD*) и вариантов использования.

Методы, ориентированные на активы, сосредоточены на идентификации активов организации, принадлежащих рассматриваемой системе. Они предполагают анализ воздействия утраты или компрометации целевых активов на систему, проводимый в соответствии с чувствительностью и ценностью данных с точки зрения потенциального злоумышленника. Специалисты определяют приоритетность выявленных угроз и рисков. Несмотря на то что подобные методы не подразумевают анализа недостатков ПО или проектирования систем, они могут быть использованы для разработки векторов атак в данной сфере. В связи с этим специалисты часто утверждают, что такие методы являются следствием подхода к проектированию, основанного на имеющемся в распоряжении организации ПО.

Методы, ориентированные на атаку, направлены на угрозы и злоумышленника. Происходит идентификация поверхности атаки – всех возможных средств, с помощью которых неизвестный злоумышленник может инициировать вектор атаки, ведущий к одному или нескольким целевым активам. В отношении поверхности атаки в дальнейшем проводятся анализ, количественная оценка риска и последующая разработка многокомпонентной политики безопасности. Следует отметить, что здесь активы не ограничиваются данными и предполагают также возможности системы и техническое обеспечение, контролируемое системой. При дополнении методами, ориентированными на атакующего, общая концепция ориентации на атаку расширяется предопределением злоумышленников, их мотивов, целей и др.

Рассмотрим самые широко применяемые методы моделирования угроз среди каждой из вышеперечисленных категорий: *STRIDE* (***s****poofing identity,* ***t****ampering of data,* ***i****nformation disclosure,* ***d****enial of service,* ***e****levation of privilege*), *PASTA* (***p****rocess for* ***a****ttack* ***s****imulation and* ***t****hreat* ***a****nalysis*) и деревья атак (*attack trees*).

STRIDE – зрелый и эффективный системно ориентированный метод моделирования угроз, разработанный в 1999 г. инженерами компании *Microsoft* для внутреннего использования [8]. Его нельзя назвать полноценным методом моделирования угроз, поскольку он является скорее их классификацией, которая учитывается при разработке ПО. Компоненты данной классификации и связанные с ними нарушенные свойства безопасности отображены в табл. 1.

Таблица 1

Категории угроз метода *STRIDE*

Table 1

***STRIDE* threat categories**

Угроза	Определение	Нарушенное свойство
Подмена личности (*spoofing identity*)	Незаконный доступ к данным, используемым для аутентификации, в целях выдать себя за легитимного пользователя	Аутентификация
Подделка данных (*tampering of data*)	Несанкционированное внесение изменений на диске, в сети, памяти и в других элементах системы	Целостность
Отказ от ответственности (*repudiation*)	Отрицание пользователем выполнения тех или иных действий	Неотказуемость
Раскрытие информации (*information disclosure*)	Предоставление информации тем, кто не должен иметь к ней доступа	Конфиденциальность
Отказ в обслуживании (*denial of service*)	Исчерпание ресурсов системы или ее компонента, которое делает его недоступным для использования	Доступность
Повышение привилегий (*elevation of privilege*)	Несанкционированное повышение уровня доступа в системе	Авторизация

Примечание. Разработано на основе [4].

В основе *STRIDE* лежит взаимодействие со структурой рассматриваемой системы, где сначала определяются объекты, события, потоки данных и границы доверия. По итогам анализа в целях визуального документирования системы разрабатываются диаграммы потоков данных, от точности которых зависит успех моделирования угроз. Последующий анализ возможности применения компонентов *STRIDE* к элементам системы используется для поиска потенциальных векторов атак и уязвимостей [4; 8].

Недостатком метода *STRIDE* является то, что он не рассчитан на генерацию и разработку мер противодействия выявленным угрозам. Также ввиду изначальной ориентации на анализ угроз ПО *STRIDE* слабо применимо для моделирования сотрудниками, не имеющими специальной подготовки в сфере разработки систем информационной безопасности.

Метод *PASTA* ориентирован на активы и предполагает сопоставление целей организации с техническими требованиями [3]. Он сосредоточен на исследовании угроз и их влияния на деятельность организации, что помогает своевременно разрабатывать соответствующие контрмеры.

Метод *PASTA* состоит из семи этапов. Подробно они представлены в табл. 2.

Таблица 2

Этапы метода *PASTA*

Table 2

***PASTA* stages**

№ п/п	Этап	Действия
1	Определение целей	• определение целей бизнеса, безопасности и соблюдения политики; • анализ воздействия на бизнес
2	Определение технического контекста	• определение границ технической среды; • выяснение зависимости инфраструктуры, приложения, ПО
3	Декомпозиция приложения	• идентификация вариантов использования, определение уровней доверия и точек входа в приложение; • идентификация участников, активов, служб, ролей, источников данных; • разработка диаграмм потоков данных и границ доверия
4	Анализ угроз	• анализ вероятных сценариев атак; • регрессионный анализ событий безопасности; • корреляция и аналитика киберугроз
5	Анализ уязвимостей	• запросы отчетов о существующих уязвимостях и отслеживание проблем; • составление карт соотношения угроз и текущих уязвимостей с помощью деревьев угроз; • анализ недостатков разработки с помощью вариантов использования и злоупотребления; • ранжирование и классификация уязвимостей
6	Моделирование атак	• анализ поверхности атаки; • развитие дерева атак, управление библиотекой атак; • анализ атак и эксплойтов с помощью деревьев атак
7	Анализ рынков	• анализ количественного и качественного воздействия на бизнес; • выявление контрмер и анализ остаточных рисков; • идентификация стратегий снижения рисков

Примечание. Разработано на основе [3].

Неоспоримым преимуществом *PASTA* является возможность его применения практически в любых учреждениях, за исключением тех, где отсутствует поддержка со стороны руководства. Важным элементом данного метода выступает анализ воздействия рисков на деятельность, что, в свою очередь, распространяет ответственность (невозможную без непосредственного участия руководителей) за безопасность на всю организацию. Более того, данный метод представляет собой полноценный фреймворк по анализу рисков, часть которого – моделирование угроз, что также является плюсом [3].

Однако указанные преимущества метода таят в себе недостатки. Так, взаимодействие с каждым элементом системы, включая руководство организации, требует проведения многочасового обучения всех ключевых участников процесса. Детальная проработка данного вопроса, выходящего за рамки моделирования угроз, несет дополнительные сложности.

Деревья атак в моделировании угроз – один из старейших и наиболее используемых методов. Ранее они выступали в качестве автономного метода моделирования, однако сегодня являются частью многих других методологий или применяются параллельно с ними [9].

Деревья атак, также называемые графами атак, представляют собой диаграммы, отображающие пути, по которым атаки могут проходить в рассматриваемой системе, где корнем дерева является цель атаки, а ветвями – способы достижения этой цели. При создании деревьев атак для моделирования угроз каждая цель злоумышленника изображена в виде дерева, которое отдельно или совместно с другими релевантными деревьями может быть разработано как для всей системы, так и для ее элементов. Пример показан на рис. 1.

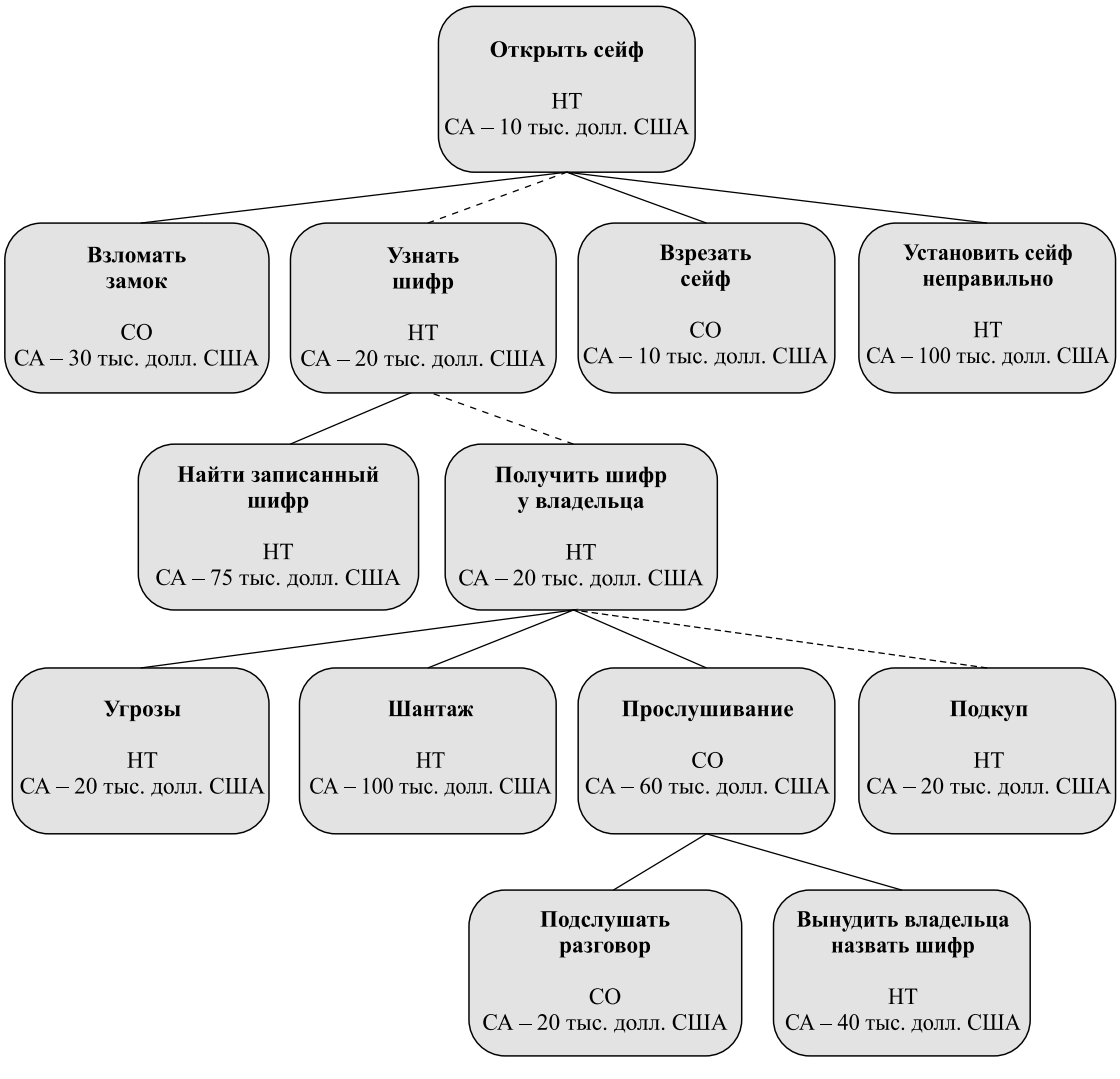


Рис. 1. Пример дерева атак:
НТ – не требует специального оборудования;
СО – требует специального оборудования;
СА – стоимость атаки, долл. США.
Источник: [9]

Fig. 1. Attack tree example:
НТ – no special equipment; СО – special equipment;
СА – attack cost, US dollars.
Source: [9]

Создание деревьев атак является сложной задачей. Каждый узел дерева необходимо проанализировать с точки зрения влияния на систему в целом, для чего используются диаграммы потока данных. В ходе моделирования оцениваются полнота графа и его возможное расширение дополнительными компонентами, исследуются альтернативные способы достижения целей моделирования. Для создания полноценной модели необходимо также документировать основные характеристики атак, такие как вероятность и стоимость, и меры противодействия, что приводит к усложнению построения модели [9]. Наконец, деревья атак не подходят для моделирования угроз на более низких уровнях системы. Данные проблемы делают метод не самым эффективным с точки зрения независимого моделирования угроз.

Таким образом, каждый из указанных методов содержит ограничения. Это соответствует отмеченному нами факту, что методы моделирования обычно не рассматривают все компоненты моделирования угроз, а ориентируются на детальную проработку одного или нескольких из них. Дополнительным ограничением методов выступает сложность, которая препятствует их использованию сотрудниками, не обладающими необходимыми знаниями и навыками в области информационной безопасности. Данные обстоятельства приводят к упущению аспектов, являющихся ключевыми для моделирования угроз и предусмотрения его возможных компонентов. Как следствие, возникает проблема разработки полноценного плана безопасности, ответных и предупредительных мер, что может угрожать информационной и экономической безопасности организации.

Авторский метод моделирования угроз на основе шаблона

Чтобы обеспечить продуктивное и полноценное моделирование угроз, метод должен отвечать трем условиям: включать структурный подход, учитывать оптимальное количество деталей и представлять данные в читаемом формате [10].

Структурный подход заключается в том, чтобы разделить большой и комплексный проект моделирования угроз на серию более мелких и управляемых модулей. Подобный подход позволяет корректно определить цель моделирования, уделить внимание деталям и провести их тщательный анализ.

Оптимальное количество деталей является решающим фактором успешного моделирования угроз. Необходимо исходить из того факта, что не все пользователи подхода являются специалистами в области информационной безопасности. Поэтому, чтобы модель оставалась понятной и легкой для восприятия и разработки, но в то же время давала возможность всесторонне оценить систему организации, в нее следует включить оптимальное количество деталей. Подобный комплексный подход увеличит вероятность успешного моделирования рисков и позволит избежать упущения угроз.

Удобочитаемость подразумевает способ представления данных в модели и влияет на то, как пользователи обрабатывают их. Если информация представлена в сложном для восприятия виде, это не позволит сосредоточиться на анализе даже при выполнении двух предыдущих условий. Поэтому метод моделирования угроз должен иметь такой формат, который позволит специалистам и простым пользователям эффективно считывать и воспринимать данные.

На основе шаблона мы разработали метод моделирования угроз, который устраняет недостатки и позволяет быстро и продуктивно провести моделирование. Структура шаблона опирается на метод, предложенный Фондом электронных рубежей. Он является гибридом нескольких методов и включает ключевые элементы моделирования угроз. Его преимуществами также выступают структурный подход к моделированию и доступность для людей с разным уровнем подготовки в сфере информационной безопасности.

Апробация метода происходила на занятиях со студентами экономического факультета БГУ в рамках дисциплин «Цифровая безопасность», «Информационная безопасность», «Бизнес-офис организации (предприятия) и интернет-маркетинг». После наблюдения за взаимодействием студентов с исходным методом и обратной связи мы внесли изменения, позволившие сделать его структуру и логику доступнее. В результате разработан шаблон, который отвечает трем указанным условиям:

- разбивает страницу на четыре компонента (характеризующие активы, злоумышленников, угрозы и анализ рисков), которые, в свою очередь, также разделяются на составляющие;
- содержит адекватную декомпозицию, которая не отвлекает внимание от собственно моделирования;
- благодаря простому визуальному и текстовому изложению позволяет пользователю понять суть структуры и метода моделирования угроз и приступить к процессу.

Результат нашей работы представлен на рис. 2.

Шаблон моделирования угроз

Разработан для

Автор

Дата

Переоценка

1. Активы

Что мы хотим защитить?
Кто или что взаимодействует с активами?
Где они находятся?
Как они защищены?

2. Злоумышленники

От кого мы защищаем активы?
Кто может хотеть совершить атаку?
Кто может неумышленно нанести вред?

3. Мотивы

Какие цели побуждают злоумышленников к совершению атаки?

4. Потенциал

На что способен злоумышленник?
Какими навыками он обладает?
Какое оборудование у него есть?

5. Угрозы

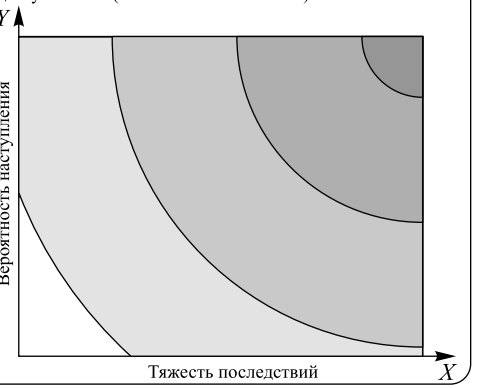
Что может сделать злоумышленник?
Что может произойти с активами?

6. Последствия

Что случится, если мы не защитим активы?
Что произойдет, если мы не справимся с атакой?
Как атака повлияет на другие активы?

7. Анализ рисков

Какова вероятность того, что нам будет необходимо защитить активы?
Оцените выявленные угрозы на карте.
Отметьте угрозы на карте и определите их приоритет по цвету области (чем темнее – тем выше).



8. Контрмеры

Что мы готовы сделать для того, чтобы предотвратить возможные последствия?
Запишите возможные меры противодействия угрозам в порядке убывания их приоритета.

Рис. 2. Шаблон моделирования угроз

Fig. 2. Threat modelling canvas

Шаблон моделирования угроз состоит из восьми блоков. В ходе заполнения шаблона мы отвечаем на вопросы, которые помогут рассмотреть каждый элемент подробно. Для упрощения некоторые компоненты были разделены или совмещены. Рассмотрим блоки шаблона в порядке их заполнения.

В блоке «активы» рассматриваются элементы системы, которые пользователи шаблона планируют или должны защитить. В отношении цифровой безопасности активами могут быть пароли, аккаунты, цифровой след, местоположение человека или группы лиц и т. д. При заполнении данного блока анализ стоит также дополнить инвентаризацией компонентов системы, взаимодействующих с активами.

При рассмотрении блока «злоумышленники» следует проанализировать, какие лица, группы лиц или организации могут (с умыслом или без него) причинить вред активам или инфраструктуре, связанной с ними. При этом стоит помнить о том, что круг злоумышленников не ограничен киберпреступниками и может включать сотрудников и членов их семей, а также другие организации.

В блоке «мотивы» мы указываем, что побуждает злоумышленника к совершению преступления.

Возможности злоумышленников следует проанализировать в блоке «потенциал». Данную категорию необходимо рассматривать с точки зрения взаимодействия с инфраструктурой и техническими умениями. Так, другие организации и хакеры могут иметь больше технических навыков, средств и специальной подготовки, но в то же время сотрудники рассматриваемой организации и члены их семей будут находиться в более тесном контакте с ней.

Блок «угрозы» включает действия, совершенные злоумышленниками, и события, приведшие к утрате или компрометации активов.

На его основании заполняется блок «последствия». При этом необходимо учитывать потенциал злоумышленников, поскольку в результате одного и того же действия, совершенного с разным потенциалом, последствия могут отличаться.

Затем следует блок «анализ рисков». Анализ рисков – субъективный процесс, нацеленный на приоритизацию выявленных рисков по убыванию. Его результат зависит от объекта, располагающего активами. Чтобы минимизировать субъективность анализа и максимизировать критическую оценку рисков, предлагаем использовать карту риска, где ось Y характеризует вероятность наступления события, а ось X – степень его тяжести. Для удобства график разделен на четыре области и содержит цветовое обозначение степени тяжести риска, т. е. пользователь шаблона может самостоятельно выбрать шкалу оценки рисков и приоритизировать их.

Заключительным этапом является заполнение блока «контрмеры», в котором необходимо определить свою готовность в защите активов или минимизировании последствий их утраты и компрометации. При этом следует учитывать ограничения финансового, технического и социального характера.

Отдельным элементом шаблона является графа о сроке переоценки модели угроз. Ее включение необходимо, поскольку основные элементы модели будут видоизменяться в зависимости от внешних и внутренних факторов.

Обучение применению метода моделирования угроз на основе шаблона

Системы информационной безопасности бесполезны, если нанести вред данным или компрометировать конфиденциальные данные посредством атак, цель которых – персонал организации. Именно поэтому неосведомленность, недостаточная образованность и отсутствие культуры безопасности персонала в области защиты данных являются фактором риска для информационной безопасности.

И поскольку цифровизация экономики требует вовлечения всех элементов организации в разработку мер безопасности, обучение моделированию угроз должно быть обязательным, оно поможет создать более целостную систему защиты данных. Так, персонал не только получит необходимые навыки для анализа угроз и связанных с ними рисков, но и сможет в полной мере осознать, что безопасность организации – это ответственность каждого сотрудника.

Поскольку апробация метода происходила в ходе занятий со студентами, мы, исходя из опыта взаимодействия и обратной связи, сформулировали подход к обучению моделированию угроз, который показал высокую эффективность.

Главная цель подхода предполагает помощь сотрудникам организации в осознании их вклада и роли в обеспечении целостной системы информационной безопасности.

Достижению поставленной цели обучения служат три основные задачи:

1) улучшить понимание персоналом важности процесса моделирования угроз и структуры шаблона моделирования угроз;

2) обеспечить сотрудников эффективным инструментом моделирования угроз для последующего применения в реальных условиях;

3) предоставить возможность практики устной презентации для персонала в процессе защиты модели угроз и получения обратной связи от коллег.

Обучение рекомендуется проводить с использованием эмпирического подхода. На занятиях участники самостоятельно работают с шаблоном моделирования угроз, разбираются в его структуре и значении основных элементов. Задача преподавателя в данном случае заключается в мотивации группы на изучение процесса моделирования угроз, а также в курировании хода семинара, помощи в анализе и систематизации полученного опыта. План занятия представлен в табл. 3.

Таблица 3

Структура эвристического семинара по обучению использованию метода моделирования угроз на основе шаблона

Table 3

Structure of a heuristic workshop on teaching how to use the canvas-based threat modelling method

Этап	Временная реализация, мин
Организационная часть: приветствие, знакомство с темой, мотивация	3
Актуализация знаний, мотивация на восприятие и осмысление нового материала, рассмотрение некоторых понятий	15
Постановка познавательной задачи «моделирование угроз в процессе обеспечения информационной безопасности организации»	5
Решение познавательной задачи с помощью инструмента «шаблон моделирования угроз»: • работа в группах: обсуждение и заполнение таблицы; • защита групповых проектов; • коллективная экспертная оценка результатов под руководством преподавателя; • общие выводы	30 15 5 5 5
Формулирование основных понятий метода моделирования угроз: • работа в группах: обсуждение и заполнение таблицы понятий; • индивидуальная работа по формулированию вариантов угроз и контрмер	15 10 5
Подведение итогов урока: • обобщение изученного материала; • рефлексия; • обратная связь	12 5 3 4

Мы выделили несколько условий наиболее эффективного обучения:

1) во время занятия его участники должны работать над общей проблемой. Это даст возможность сравнить и оценить завершенные проекты, стимулируя обмен конструктивной обратной связью между коллегами, и прийти к общим выводам о применении нового метода моделирования угроз;

2) в ходе семинара следует разделить участников на группы, в которых они будут прорабатывать заданную проблему. Каждый будет иметь возможность высказать свою точку зрения и принять участие в командной работе над проектом;

3) эффективным является привлечение к участию в занятии специалиста организации по обеспечению информационной безопасности или защите персональных данных (в качестве помощника преподавателя или куратора семинара), что создаст основу для лучшего понимания проблемы. Подобная практика также служит эффективным способом генерации и обмена идеями по совершенствованию системы информационной безопасности организации между представителями ее структурных элементов.

Стоит отметить, что проведение занятия не требует предварительной теоретической подготовки, поскольку его участники смогут дать определение основным понятиям самостоятельно с помощью шаблона моделирования угроз. Тем не менее наличие ранее полученных теоретико-методологических знаний в области обеспечения цифровой безопасности и защиты личных данных часто позволяет сформулировать более точное содержание структурных элементов модели. Таким образом, оптимально проводить семинар после овладения базовыми понятиями цифровой и информационной безопасности.

На наш взгляд, после основной фазы занятия необходимо провести групповое обсуждение, в процессе которого участники семинара смогут проанализировать свой опыт обучения, преобразуя полученную информацию для рефлексивной деятельности.

Апробация подхода во время занятий со студентами и сбора обратной связи показала, что его цели достигнуты. В данный момент нельзя ответить на вопрос, достигнет ли предложенный подход своих целей при обучении сотрудников организации, но мы предполагаем, что дальнейшее внедрение метода моделирования угроз в практику покажет его эффективность.

Заключение

Таким образом, рассмотрены основные категории методов моделирования угроз, проанализированы особенности и недостатки часто применяемых методов. Многие методы моделирования угроз содержат ограничения, поскольку либо ориентированы на детальную проработку конкретных элементов систем, либо выходят за рамки процесса моделирования. Это, в свою очередь, приводит к упущению аспектов, являющихся ключевыми для моделирования угроз и предусмотрения его возможных компонентов. Существует проблема разработки полноценного плана безопасности и ответных и предупредительных мер, что может привести к угрозам информационной и экономической безопасности организации.

Разработан метод моделирования угроз, основанный на шаблоне, который позволяет провести быстрый и продуктивный процесс моделирования, доступный для людей с разной подготовкой в сфере информационной безопасности. Предложенный метод включает ключевые элементы моделирования угроз и использует структурный подход. Сформулированы структура семинара, который может быть использован при обучении моделированию угроз, и требования к нему.

В будущем мы планируем апробировать предложенный нами метод в организации для анализа потенциальных угроз информационных и бизнес-систем. Мы также намерены рассмотреть один из перечисленных путей научной и практической разработки шаблона, заключающийся в его применении в процессе обучения сотрудников основам цифровой безопасности и защите персональных данных.

Библиографические ссылки

1. Parenty TJ, Domet JJ. *Leader's guide to cybersecurity: Why boards need to lead – and how to do it.* Boston: Harvard Business Review Press; 2019. 240 p.

2. Макаревич ВА, Минюкович ЕА, Мулярчик КС. Проблемы информационной безопасности при организации удаленной работы сотрудников. *Актуальные проблемы науки XXI века* [Интернет]. 2020 [процитировано 10 января 2020 г.];9:12–16. Доступно по: http://library.miu.by/journals!/item.science-xxi/issue.9/article.2.html.

3. UcedaVelez T, Morana MM. *Risk centric threat modelling: process for attack simulation and threat analysis.* Hoboken: John Wiley & Sons; 2015. 696 p.

4. Shostack A. *Threat modelling: designing for security*. Hoboken: John Wiley & Sons; 2014. 624 p.

5. Jaatun MG, Bernsmed K, Cruzes DS. Threat modelling in agile software development. In: Felderer M, Scandariato R, editors. *Exploring security in software architecture and design.* Hershey: IGI Global; 2019. p. 1–14. DOI: 10.4018/978-1-5225-6313-6.ch001.

6. Makarevich UA. Ethical hacking and social engineering. Legal ways of protecting business. В: Берлинская СГ, редактор. *Сборник работ 73-й научной конференции студентов и аспирантов Белорусского государственного университета; 16–25 мая 2016 г.; Минск, Беларусь. Часть 2.* Минск: БГУ; 2016. с. 121–125.

7. Jouini M, Rabai LBA. Threats classification: state of the art. In: *Handbook of research on modern cryptographic solutions for computer and cyber security*. Hershey: IGI Global; 2016. p. 368–392. DOI: 10.4018/978-1-5225-0105-3.ch016.

8. Hernan S, Lambert S, Ostwald T. Uncover security design flaws using the STRIDE approach. *MSDN Magazine* [Internet]. 2006 [cited 2021 January 10]. Available from: https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach.

9. Schneier B. Attack trees. In: Schneier B. *Secrets and lies: digital security in a networked world.* Hoboken: John Wiley & Sons; 2015. p. 318–333. DOI: 10.1002/9781119183631.ch21.

10. Krishnan S. *A hybrid approach to threat modelling* [Internet] 2017. [cited 2021 January 10]. Available from: https://www.researchgate.net/publication/320183133_A_Hybrid_Approach_to_Threat_Modelling_A_Hybrid_Approach_to_Threat_Modelling. DOI: 10.13140/RG. 2.2.33303.88486.

References

1. Parenty TJ, Domet JJ. *Leader's guide to cybersecurity: Why boards need to lead — and how to do it.* Boston: Harvard Business Review Press; 2019. 240 p.

2. Makarevich UA, Miniukovich KA, Mulyarchik KS. Information security issues in the organisation of remote work of employees. *Current issues of science in the 21st century* [Internet]. 2020 [cited 2021 January 10];9:12–16. Available from: http://library.miu.by/journals!/item.science-xxi/issue.9/article.2.html. Russian.

3. UcedaVelez T, Morana MM. *Risk centric threat modelling: process for attack simulation and threat analysis.* Hoboken: John Wiley & Sons; 2015. 696 p.

4. Shostack A. *Threat modelling: designing for security*. Hoboken: John Wiley & Sons; 2014. 624 p.

5. Jaatun MG, Bernsmed K, Cruzes DS. Threat modelling in agile software development. In: Felderer M, Scandariato R, editors. *Exploring security in software architecture and design.* Hershey: IGI Global; 2019. p. 1–14. DOI: 10.4018/978-1-5225-6313-6.ch001.

6. Makarevich UA. Ethical hacking and social engineering. In: Berlinskaya SG, editor. *Sbornik rabot 73-i nauchnoi konferentsii studentov i aspirantov Belorusskogo gosudarstvennogo universiteta; 16–25 maya 2016 g.; Minsk, Belarus'. Chast' 2* [Collection of works of 73rd scientific conferences of students and postgraduates of the Belarusian State University; 2016 May 16–25; Minsk, Belarus. Part 2]. Minsk: Belarusian State University; 2016. p. 121–125.

7. Jouini M, Rabai LBA. Threats classification: state of the art. In: *Handbook of research on modern cryptographic solutions for computer and cyber security*. Hershey: IGI Global; 2016. p. 368–392. DOI: 10.4018/978-1-5225-0105-3.ch016.

8. Hernan S, Lambert S, Ostwald T. Uncover security design flaws using the STRIDE approach. *MSDN Magazine* [Internet]. 2006 [cited 2021 January 10]. Available from: https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach.

9. Schneier B. Attack trees. In: Schneier B. *Secrets and lies: digital security in a networked world.* Hoboken: John Wiley & Sons; 2015. p. 318–333. DOI: 10.1002/9781119183631.ch21.

10. Krishnan S. *A hybrid approach to threat modelling* [Internet] 2017. [cited 2021 January 10]. Available from: https://www.researchgate.net/publication/320183133_A_Hybrid_Approach_to_Threat_Modelling_A_Hybrid_Approach_to_Threat_Modelling. DOI: 10.13140/RG.2.2.33303.88486.

Статья поступила в редколлегию 05.02.2021.
Received by editorial board 05.02.2021.