DOI: 10.25728/mlsd.2023.1240

МЕТОДИКА ОЦЕНКИ РИСКА EBIOS

Черняев М.Д.
Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
Paladine777@gmail.com

Аннотация. Цель статьи заключается в рассмотрении особенностей французской методики оценки рисков EBIOS. В ходе работы разобран способ использования данной методики и описан используемый подход. Это позволяет сделать выводы об удобности и области применения системы EBIOS, а также о рациональности применения итеративного подхода в целом.

Ключевые слова: риск, анализ, безопасность, итеративный, сценарии, кибератака, экосистема.

Введение

В данной работе проводится исследование и тестирование системы анализа риска EBIOS. В настоящее время качественная оценка риска необходима для надежного функционирования любой информационной системы. Существует значительное количество методик, призванных упростить и систематизировать процесс оценки рисков, однако в данной работе предлагается ознакомиться конкретно с принципами работы метода EBIOS.

В результате проведенного исследования будет продемонстрирована работа пяти этапов EBIOS и доказана эффективность данного метода подхода к оценке рисков.

Объект исследования – организация, нуждающаяся в защите.

Предмет исследования – система анализа риска EBIOS.

Данная система очень мало изучена в современных исследованиях из-за ее относительной новизны и достаточно локального использования на территории франкоговорящих стран.

1. Обзор метода

EBIOS Risk Manager (EBIOS RM) — это метод оценки и обработки цифровых рисков, опубликованный национальным агентством кибербезопасности Франции (ANSSI) при поддержке Club EBIOS. Он обеспечивает набор инструментов, который можно адаптировать, использование которого варьируется в зависимости от цели проекта и который совместим с действующими эталонными стандартами с точки зрения управления рисками, а также с точки зрения кибербезопасности.

EBIOS RM позволяет оценивать цифровые риски и определить меры безопасности, которые необходимо предпринять для их контроля. Это также позволяет подтвердить приемлемый уровень риска и в долгосрочной перспективе придерживаться подхода непрерывного улучшения. Наконец, этот метод позволяет использовать ресурсы и аргументы, полезные для общения и принятия решений внутри организации и в отношении ее партнеров.

Метод EBIOS RM можно использовать для нескольких целей:

- создание или укрепление процесса управления цифровыми рисками в организации;
- оценка и обработка рисков, связанные с цифровым проектом, в частности, с целью аккредитации безопасности;
- определение уровня безопасности, который должен быть достигнут для продукта или услуги, в соответствии с его вариантами использования и рисками, которым необходимо противодействовать, как то, с точки зрения сертификации или аккредитации.

Это применимо как к государственным, так и к частным организациям, независимо от их размера, сферы деятельности и того, разрабатываются ли их информационные системы или уже существуют.

Также стоит отметить, что инструментарий EBIOS находится в открытом доступе и распространяется бесплатно, что делает систему доступнее. Минусом является то, что на данный момент EBIOS поддерживает только французский язык, однако разработчики недавно упоминали, что планируют перевод на английский.

2. Подход пяти шагов

Метод EBIOS Risk Manager использует подход к управлению цифровыми рисками, начиная с самого высокого уровня (основные задачи изучаемого объекта) и постепенно доходя до бизнес- и технических функций путем изучения возможных сценариев риска. Он направлен на вырабатывание синтеза между

«соблюдением требований» и «сценариями», размещая эти два взаимодополняющих подхода так, чтобы максимизировать их эффективность.

Подход на основе соответствия используется для определения базовых требований безопасности, на которых основан подход для разработки узконаправленных или комплексных сценариев риска. Это предполагает, что случайные риски и риски окружающей среды априори обрабатываются с помощью подхода, основанного на соблюдении базовых требований безопасности. Исходя из этого, оценка рисков с помощью сценариев, описанных методом EBIOS, фокусируется на преднамеренных угрозах.

EBIOS — это метод, который можно адаптировать. Он представляет собой удобный набор инструментов, из которого выполняемые действия, их уровень детализации и их последовательность легко адаптировать под желаемый метод использования. Способ применения метода различается в зависимости от изучаемого предмета, ожидаемых результатов, степени изученности периметра исследования или сектора, к которому он применяется. Итеративность метода выражается в том, что некоторые его этапы подразумевают постоянное обновление путем повторного анализа и дополнения данных. Нижеследующая таблица предлагает варианты использования в соответствии с целевой задачей.

Таблица 1. Варианты использования шагов метода EBIOS

		Главные секции, которые нужно применить				
Цель исследования		1	2	3	4	5
Определить базовые требования безопасности, применимые к изучаемому объекту		X				
Соответствовать эталонным стандартам цифровой безопасности		X				X
Оценить уровень угрозы экосистеме по отношению к изучаемому объекту				X(1)		
Определить и проанализировать сценарии высокого уровня, интегрирующие в экосистему			X	X		
Провести предварительное исследование рисков, чтобы определить приоритетные направления для улучшения безопасности		X(2)	X	X		X(3)
Провести полное и тщательное исследование рисков, например, в отношении продукта безопасности или с целью аккредитации системы		X	X	X	X	X
Организовать аудит безопасности и, в частности, пентест				X	X	
Организовать системы обнаружения и реагирования, например, на уровне оперативного центра безопасности (ОЦБ)				X	X	

1: только этап a) секции; не требуется предварительное проведение семинаров 1 и 2.

2: в рамках предварительного исследования степень глубины секции 1 должна быть адаптирована (например, перечисление лишь бизнес-активов, проведение общего анализа базовых требований безопасности).

3: только этап b) секции 5.

Шаг 1: Область действия и базовые требования безопасности

Первый шаг направлен на определение изучаемого объекта, участников семинаров и временных рамок. В течении этого шага перечисляются миссии, бизнес-активы и вспомогательные активы, связанные с изучаемым объектом.

Определяются опасные события, связанные с бизнес-активами, и оценивается серьезность их последствий. Также определяются базовые требования безопасности и дифференциал.

Шаг 1 позволяет следовать подходу «соблюдение требований», соответствующему первым двум этапам пирамиды управления цифровыми рисками, и рассматривать исследование с точки зрения «защиты».

Целью первого шага является определение структуры исследования, его деловой и технической сферы, связанных с ними опасных событий и базовых требований безопасности. Этот шаг является предварительным условием для проведения оценки рисков. Период, который следует рассматривать для этого шага, совпадает со стратегическим циклом.

Шаг 2: Источники рисков

На втором шаге определяются и характеризуются источники риска (ИР) и их цели высокого уровня, называемые целевыми задачами (ЦЗ). Это должно ответить на следующий вопрос: кто или что может посягать на миссии и бизнес-активы, определенные на секции, и с какими целями?

Затем источники риска и целевые задачи охарактеризованы и оценены, чтобы сохранить наиболее важные из них. Они будут полезны для построения сценариев для секций 3 и 4. В конце этого шага выбираются наиболее подходящие пары ИР/ЦЗ. Результаты формализуются в составлении карты источников риска.

Шаг 3: Стратегические сценарии

На шаге 3 получается четкое представление об экосистеме и налаживается картографирование цифровой угрозы последней по отношению к изучаемому объекту.

Это позволяет создавать высокоуровневые сценарии, называемые стратегическими сценариями.

Они представляют собой пути атаки, которые источник риска может использовать для достижения своей цели. Эти сценарии разрабатываются в масштабе экосистемы и бизнес-активов изучаемого объекта. Их оценивают по степени тяжести. В конце этого шага вы уже можете определить меры безопасности в экосистеме.

Шаг 3 следует рассматривать как предварительное исследование рисков. Это может привести к определению мер безопасности, которые необходимо применять в отношении экосистемы. Стратегические сценарии, выбранные на шаге 3, составляют основу сценариев операций для шага 4.

Шаг 4: Сценарии операций

Целью шага 4 является создание технических сценариев, включающих методы атаки, которые, вероятно, будут использоваться источниками риска, для реализации стратегических сценариев. На этом шаге используется подход, аналогичный подходу предыдущей секции, но основное внимание уделяется критически важным вспомогательным активам. Затем оценивается уровень вероятности воплощения в жизнь полученных операционных сценариев. Период, который следует рассматривать для данного шага, является периодом операционного цикла

Примечания: Данные шагов 3 и 4 естественным образом пополняются во время последовательных итераций.

Шаги 2, 3 и 4 позволяют оценить риски, что составляет последний этап пирамиды управления цифровыми рисками. Они используют базовые требования безопасности в соответствии с различными путями атак, которые напрямую исходят из рассматриваемых угроз и число которых ограничено для облегчения анализа.

Шаг 5: Обработка рисков

Последний шаг заключается в составлении сводки всех изученных рисков для определения стратегии обработки рисков. Последняя затем разбивается на конкретные меры безопасности, записанные в план непрерывного усовершенствования. В ходе этого шага составляется сводка остаточных рисков и определяется основа для мониторинга рисков.

Обновление исследования рисков осуществляется в соответствии с запланированными стратегическими и операционными циклами. В случае крупных событий, ставящих под сомнение

актуальность сценариев (появление новой угрозы, существенное изменение в экосистеме или изучаемом объекте и т. д.), сценарии будут подлежать актуализации до нужного уровня.

3. Заключение

В результате проведения анализа рисков по методу EBIOS была создана картина рисков и предложены сценарии их контроля и предотвращения.

В данной работе было проведено исследование и тестирование метода анализа риска EBIOS.

В результате проведенного исследования была продемонстрирована работа пяти этапов EBIOS и доказана эффективность данной системы.

Благодаря высокой степени персонализации и интуитивно понятной системе, методика оценки риска EBIOS является удобной основой для выстраивания структуры оценки риска и ее дальнейшей сертификации и эксплуатации.

Литература

1. *Wissam Abbass, Amine Baina, Mostafa Bellafkih*. Using EBIOS for risk management in critical information infrastructure – 5th World Congress on Information and Communication Technologies (WICT) Year: 2015 |Conference Paper | Publisher: IEEE URL: https://ieeexplore.ieee.org/document/7489654 (дата обращения 9.10.2022).
2. *John Mcdonald; Nouha Oualha; Armaud Puccetti; Artur Hecker* Application of EBIOS for the risk assessment of ICT use in electrical distribution sub-stations; Frederic Planchon 2013 IEEE Grenoble Conference Year: 2013 | Conference Paper | Publisher: IEEE URL: https://ieeexplore.ieee.org/document/6652221 (дата обращения 11.10.2022).
3. *Berrehili Fatima Zahra, Belmekki Abdelhamid* Risk analysis in Internet of Things using EBIOS 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)URL: (дата обращения 12.10.2022).
4. *Hicham Elachgar; Boubker*. Information security, new approach Regragui Second International Conference on the Innovative Computing Technology (INTECH 2012) Year: 2012 | Conference Paper | Publisher: IEEE Cited by: Papers (2) URL: https://ieeexplore.ieee.org/document/6457815 (дата обращения 13.10.2022).
5. *Omar EL IDRISSI; Abdellatif MEZRIOUI; Abdelhamid BELMEKKI*. A lightweight risk analysis of a critical infrastructure based ICSs 2019 1st International Conference on Smart Systems and Data Science (ICSSD) Year: 2019 | Conference Paper | Publisher: IEEE URL: https://ieeexplore.ieee.org/document/9002902 (дата обращения 14.10.2022).