– 2020. – Vol. 14. Issue: 4. – P. 4684-4693. – DOI: 10.1109/JSYST.2020.2970748.

12. *Iskhakov A., Meshcheryakov R.* Intelligent System of Environment Monitoring on the Basis of a Set of IOT-Sensors / International Siberian Conference on Control and Communications (SIBCON). – Tomsk, 2019. – P. 1-5. – DOI: 10.1109/SIBCON.2019.8729628.

13. *Zeadally S., Adi, E., Baig Z., Khan I.A.* Harnessing artificial intelligence capabilities to improve cybersecurity // IEEE Access. – 2020. – Vol. 8. – Article 8963730. – P. 23817-23837. – DOI: 10.1109/ACCESS.2020.2968045.

14. *Ge X.H., Han Q.L., Zhang X.M., Ding D.., & Yang F.W.* Resilient and secure remote monitoring for a class of cyber-physical systems against attacks // Information Sciences. – 2020. – Volume 512. – P. 1592-1605. – DOI: 10.1016/j.ins.2019.10.057.

15. *Nikolai Fomin, Roman V. Meshcheryakov*. Digital Twin Security of the Cyber-Physical Water Supply System / Handbook of Digital Twins. – CRC Press, 2024. – 1040 p. (in print).

DOI: 10.25728/iccss.2023.65.26.042

Черняев М.Д.

Сравнение методов оценки риска ФСТЭК и EBIOS

Аннотация: Целью данной работы является сравнение двух методов оценки риска: EBIOS и ФСТЭК. EBIOS публикуется Национальным агентством кибербезопасности Франции (ANSSI), а ФСТЭК был разработан в России. Оба метода используются относительно локально, но уже доказали свою эффективность во Франции и России соответственно. В данной работе приводится краткое описание этих методов и их сравнение. Приведенное ниже исследование носит субъективный характер, и автор сравнивает эти методы, исходя из своих личных предпочтений, поскольку других подобных сравнений ранее не производилось. В ходе исследования дается краткое описание и сравнение обоих методов, поскольку оба имеют свои плюсы и минусы, и могут оказаться более

эффективными в конкретной ситуации. В результате можно сделать вывод, что применение обоих методов может оказаться эффективным, и главная задача состоит в том, чтобы выбрать наиболее подходящий для конкретной ситуации подход.

Ключевые слова: риск, оценка риска, итеративный подход, кибер-атаки, безопасность

Введение

В данной работе демонстрируются методы оценки рисков EBIOS и FSTEC. Следует заранее отметить, что сами эти методы не являются программными или аппаратными средствами, а представляют собой своего рода план или стандарт для тех, кто занимается оценкой рисков. В настоящее время развитая система оценки рисков является критически важной для надежного функционирования любой информационной инфраструктуры. Для упрощения и систематизации процесса оценки рисков разработано значительное количество таких систем. В данной статье дается обзор работы методов EBIOS и ФСТЭК, после чего проводится их сравнение.

В ходе исследования будут рассмотрены плюсы и минусы каждого метода, выделены их особенности. Объектом исследования являются методы оценки рисков EBIOS и FSTEC. Предметом исследования является сравнение этих двух методов. Эти методы не обладают общемировой известностью из-за относительно локального использования их во франко- и русскоязычных странах соответственно.

Обзор метода EBIOS

EBIOS Risk Manager – это метод оценки и обработки цифровых рисков, опубликованный Национальным агентством кибербезопасности Франции (ANSSI). Данный подход представляет собой набор из пяти шагов, который может быть скорректирован в зависимости от поставленной задачи, и совместим с современными эталонными стандартами как с точки зрения управления рисками, так и с точки зрения кибербезопасности [1].

EBIOS позволяет провести оценку цифровых рисков и после этого определить необходимые меры безопасности. Он также

позволяет определить разумную степень риска и в долгосрочной перспективе следовать подходу постоянного совершенствования. Кроме того, этот метод упрощает процессы коммуникации и принятия решений как для организации, так и для ее партнеров.

С помощью подхода EBIOS можно достичь нескольких целей. Например, создать или укрепить систему оценки цифровых рисков в организации, определить желаемый уровень безопасности продукта или услуги в зависимости от сферы использования и потенциальных рисков, которым необходимо будет противостоять и т.п.

Метод EBIOS применим к государственным и частным организациям, независимо от их размера, сферы деятельности и состояния информационных систем.

Следует также отметить, что инструментарий некоторых существующих систем, использующих подход EBIOS, находится в открытом доступе, что делает его более доступным. Недостатком является то, что в настоящее время большая часть документации по EBIOS доступна только на французском языке. Однако не так давно был сделан перевод на английский язык основных принципов EBIOS [2], что потенциально может привести к большему признанию в ближайшее время.

Подход, основанный на пяти шагах

Метод EBIOS Risk Manager подходит к управлению цифровыми рисками, начиная с верхнего уровня (основные цели изучаемого объекта) и постепенно доходя до практических функций путем исследования потенциальных сценариев риска. Главной целью является разработка симбиоза «соблюдения требований» и «адаптации к событиям», при котором эти два взаимодополняющих подхода будут сбалансированы таким образом, чтобы их эффективность максимально повысилась.

Подход «соблюдения требований» используется для определения базовых требований безопасности с целью разработки узконаправленных или сложных сценариев рисков. Этот подход предполагает, что случайные и природные риски устраняются в рамках базовых требований безопасности. По сути, это означает, что сценарии оценки рисков, изучаемые методом EBIOS, ориентированы только на преднамеренные угрозы [3].

В основе метода EBIOS лежат пять шагов.

1. Область применения и базовые требования безопасности (их определение).

2. Источники рисков (их определение).

3. Стратегические сценарии (определение масштабного плана действий злоумышленников, составление пар из источника риска и его целевой задачи).

4. Сценарии операций (разбитие стратегических сценарий на конкретные операции, разбор этих операций).

5. Обработка рисков (составление сводки всех изученных рисков для определения стратегии обработки рисков).

EBIOS – это подход, который легко адаптируется и персонализируется. Он представляет собой удобный конструктор, состоящий из отдельных шагов, некоторые из которых могут быть опущены или повторены в зависимости от текущей цели. Например, если поставлена задача определить базовые требования безопасности, применимые к изучаемому объекту, то хватит лишь первого шага. Если же необходимо провести полное и тщательное исследование рисков, то потребуются все пять шагов [4]. Способы применения метода варьируются в зависимости от изучаемого объекта, ожидаемых результатов и масштабов исследования или сферы деятельности объекта. Итерационный характер метода проявляется в том, что некоторые его шаги предполагают постоянное обновление путем повторного анализа и дополнения данных. Эти шаги образуют два цикла: стратегический цикл (при котором исследование проводится полностью с первого и до пятого шага, как правило, когда необходимо целиком обновить систему оценки рисков и все связанные с ней данные) и цикл операций (при котором повторно исследуются третий, четвертый и пятый шаги, т.е. источники риска и базовые требования не поменялись, однако у злоумышленников появились новые способы воплотить свои планы в жизнь).

Обзор метода ФСТЭК

Подход к оценке рисков ФСТЭК определяет порядок и содержание исследования по выявлению угроз информационной безопасности, которые могут возникнуть в информационных системах, а также по разработке моделей угроз информационной

безопасности систем и сетей. Подход ФСТЭК к управлению рисками используется для выявления угроз информационной безопасности, реализация которых возможна как в государственных и муниципальных информационных системах, так и в информационных системах персональных данных, значимых объектах критической информационной инфраструктуры Российской Федерации и т.д. [5]. Как и в случае с EBIOS, подход ФСТЭК ориентирован на оценку техногенных угроз информационной безопасности, возникновение которых обусловлено действиями злоумышленников.

Модели угроз информационной безопасности систем и сетей, разработанные и утвержденные до утверждения данной методики и без ее учета, остаются в силе. Они подлежат изменению в соответствии с этим подходом при развитии (модернизации) соответствующих систем и сетей [6]. Разработанные отраслевые (ведомственные, корпоративные) методики оценки угроз информационной безопасности не должны противоречить положениям ФСТЭК. Общая схема оценки угроз информационной безопасности в соответствии с подходом ФСТЭК состоит из трех последовательных этапов.

1. Определение негативных последствий от реализации (возникновения) угроз безопасности информации.

2. Определение возможных объектов воздействия угроз безопасности информации.

3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности (состоит из трех масштабных подэтапов, которые необходимы для формирования наиболее полной картины среды рисков: определение источников угроз безопасности информации, оценка способов реализации угроз безопасности информации и оценка актуальности угроз безопасности информации).

На всех этапах подхода ФСТЭК эксперты сверяются с исходными данными для работы над конкретным этапом, список которых приведен в официальном методическом документе. Теоретически этапы можно попробовать использовать отдельно друг от друга, однако напрямую инструкций к этому в методическом документе нет [7], что затрудняет расчет целесообразности такого подхода. Кроме того, подход ФСТЭК

расписан весьма подробно, что может помочь неуверенному начинающему пользователю, однако такая формализация процесса может негативно повлиять на гибкость подхода и возможности его персонализации.

Заключение

В результате сравнения подходов к оценке рисков EBIOS и ФСТЭК можно отметить, что если ФСТЭК представляет собой более широкий и всеобъемлющий стандарт, то EBIOS оказывается более удобным при оперативном решении локальных задач. Кроме того, подход, основанный на пяти шагах, является очень интуитивно понятным и простым «чертежом» для оценки рисков. Он может быть использован для сертификации не только всей системы оценки рисков, но и средств, направленных на решение менее комплексных задач, таких как описание среды рисков. Хотя ФСТЭК имеет крепкую основу в виде подробной структуры и множества подкрепляющих ее материалов, ему, к сожалению, не хватает гибкости и возможностей персонализации, которыми обладает EBIOS. В заключение можно сказать, что ФСТЭК – действенный, но отчасти устаревший подход, который иногда может слишком ограничивать эксперта рамками стандартизированных процедур. EBIOS же предоставляет широкие возможности для модификации и персонализации, при необходимости повторяя или даже полностью опуская некоторые из своих этапов. Именно поэтому, по мнению автора, подход EBIOS и подобные ему итеративные подходы выглядят более перспективно в современных реалиях. Это не означает, что подход ФСТЭК является неэффективным или безнадежно устаревшим, но для большей простоты и гибкости его использования было бы весьма полезно имплементировать итеративный подход и в рамках методического документа описать возможности его персонализации под нужды конкретного исследования.

Литература:

1. *Abbass W., Baina A. and Bellafkih M.* ”Using EBIOS for risk management in critical information infrastructure” / 5th World Congress on Information and Communication Technologies (WICT). – Marrakech, Morocco, 2015. – P. 107-112.

2. ANSS I-PA-048-EN, Version 1.0, November 2019.

3. *Zahra B.F. and Abdelhamid B.* “Risk analysis in Internet of Things using EBIOS” / IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). – Las Vegas, NV, USA, 2017. – P. 1-7. – DOI: 10.1109/CCWC.2017.7868444.

4. *Esselin F., Coulon K.* “EBIOS risk manager: accessible methodology to secure digital transformation”// Les Notes du CREOGN. – 2021. – № 62. – P. 1-4.

5. *Sokolov S.S., Alimov O.M., Golubeva M.G., Burlov V.G. and Vikhrov N.M.* “The automating process of information security management” / IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – Moscow and St. Petersburg, Russia, 2018. – P. 124-127. – DOI: 10.1109/EIConRus.2018.8317045.

6. *Kuzmina U., Kazakov O. and Erushev B.* “Building an Attack Tree for Analysis of Information Security Risks” / International Russian Smart Industry Conference (SmartIndustryCon). – Sochi, Russian Federation, 2023. – P. 164-168. – DOI: 10.1109/SmartIndustryCon57312.2023.10110738.

7. Методический документ от 5 февраля 2021 г. «Методика оценки угроз безопасности информации». – М.: Федеральная служба по техническому и экспортному контролю, 2021. – 83 с.

_____

_____