DOI 10.37882/2223–2966.2021.09.25

МЕТОДИКИ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ[1]

Чернов Денис Владимирович
Соискатель, Тульский Государственный Университет
cherncib@gmail.com

Аннотация. В современном мире широкое применение нашли технологии автоматизации промышленных процессов. Автоматизированные системы управления технологическими процессами (АСУ ТП) стали важной частью предприятий, функционирующих в различных сферах экономики и жизнеобеспечения по всему миру. Однако высокие темпы роста числа средств автоматизации остро поднимают проблему обеспечения информационной безопасности АСУ ТП от внешних и внутренних угроз. В настоящей работе автором проводится анализ методики оценки угроз безопасности информации ФСТЭК России и международной методики TRIKE. Анализ методик направлен на выявление общих подходов к определению источников угроз, тактик и техник оценки угроз безопасности информации, а также выявление отличий между ними, в целях применения унифицированного подхода к моделированию угроз информационной безопасности АСУ ТП.

Ключевые слова: автоматизированные системы управления, информационная безопасность, угроза, оценка угроз, модель угроз.

METHODS FOR ASSESSING INFORMATION SECURITY THREATS OF AUTOMATED PROCESS CONTROL SYSTEMS[2]

D. Chernov

Summary. In the modern world, industrial process automation technologies have found wide application. Automated process control systems (APCs) have become an important part of enterprises operating in various sectors of the economy and life support around the world. However, the high growth rates of the number of automation tools acutely raise the problem of ensuring the information security of automated process control systems from external and internal threats. In this paper, the author analyzes the methodology for assessing information security threats of the FSTEC of Russia and the international TRIKE methodology. The analysis of the methods is aimed at identifying common approaches to determining the sources of threats, tactics and techniques for assessing threats to information security, as well as identifying differences between them, in order to apply a unified approach to modeling threats to information security of automated control systems.

Keywords: automated control systems, information security, threat, threat assessment, threat model.

Введение

В процессе функционирования промышленных систем на средства автоматизации влияет множество внешних факторов и информационных воздействий, что может приводить к прогнозируемым и непрогнозируемым последствиям. Негативные информационные воздействия рассматриваются специалистами в области обеспечения информационной безопасности как потенциальные угрозы, которые могут быть реализованы нарушителями в отношении АСУ ТП. В целях снижения возможных убытков от деструктивных действий нарушителей информационной безопасности необходимо проводить мероприятия по оценке угроз безопасности информации.

Угрозы безопасности информации

В нормативно-правовой базе, регулирующей вопросы информационной безопасности и научных работах профильных специалистов, изложено множество дефиниций термина УБИ. В Таблице 1 представлено сравнение определения «угроза безопасности информации (УБИ)» из различных источников.

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (Грант ИБ) в рамках научного проекта № 15/2020.
[2] The reported study was funded by Russian Ministry of Science (information security), project number 15/2020.

Таблица 1. Сравнение определений УБИ

Источник	Определение
ГОСТ Р 50922–96 Защита информации. Основные термины и определения[1]	Совокупность условий и факторов, создающих опасность нарушения информационной безопасности.
Методика оценки угроз безопасности информации. ФСТЭК России. От 05.02.2021 г. [2]	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
Хорев А.А. Угрозы безопасности информации [3]	Совокупность условий и факторов (явлений, действий или процессов), создающих потенциальную или реально существующую опасность, в результате которой возможны утечка информации, неправомерное модифицирование (искажение, подмена), уничтожение информации или неправомерное блокирование доступа к ней.
Доктрина информационной безопасности Российской Федерации [4]	Совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.
ГОСТ Р ИСО/МЭК 27002–2012 [5]	Потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации.
Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [6]	Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при их обработке в информационной системе.
TRIKE [7]	Корень дерева атак в более крупном графике атак.

Таблица 2. Сравнительная характеристика методик оценки УБИ

Критерии	Методика	
	Методика ФСТЭК РФ	TRIKE
Входные данные	Риски	Активы, операции, атаки, правила, угрозы
Механизмы управления	Нормативные акты, техническая и эксплуатационная документация, технологические процессы, договоры использования внешней инфраструктуры (аутсорсинг), банк данных УБИ, векторы атак	Нормативные акты, техническая и эксплуатационная документация, технологические процессы
Механизмы исполнения	Экспертная группа, программные средства	Экспертная группа, программные средства, аппаратные средства
Перечень угроз	Общий перечень УБИ, содержащийся в банке данных УБИ ФСТЭК РФ bdu.fstec.ru	Генерация угроз экспертной группой
Шаблоны (векторы) компьютерных атак	Базы данных: CAPEC, ATT&CK, OWASP, STIX, WASC и др.	Генерируемое аппаратными средствами Дерево атак
Оценка рисков	Результаты оценки рисков используются при оценке угроз	По результатам оценки угроз
Результаты оценки угроз	Отражаются в модели угроз	Отражаются в модели угроз
Наличие программной реализации	Отсутствует	Есть

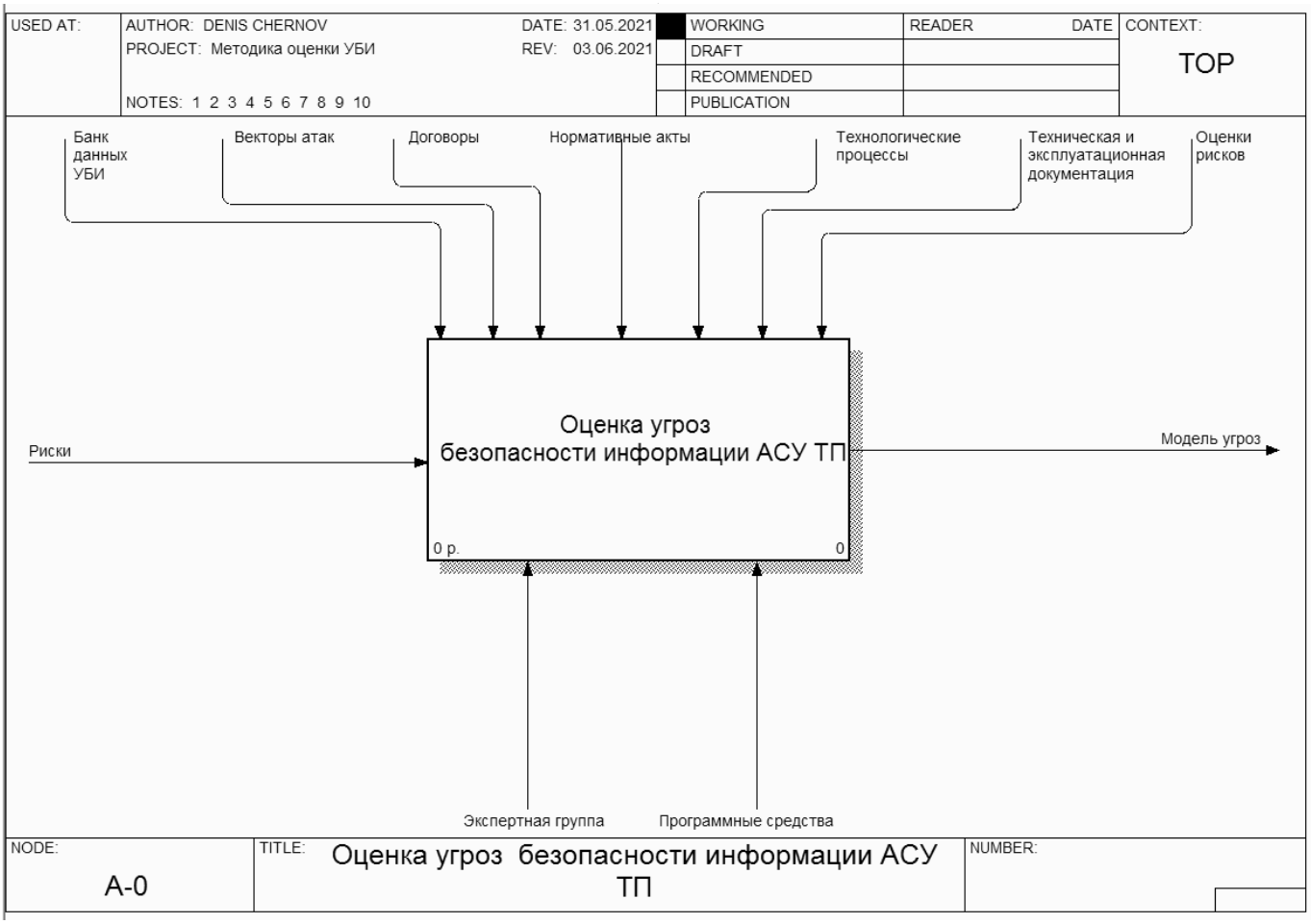


Рис. 1. IDEF0-модель методики ФСТЭК РФ

Исходя из сведений, представленных в таблице, можно сделать вывод о сходстве большинства определений УБИ из рассмотренных источников.

Методики оценки УБИ

Существует множество международных и отечественных методик оценки совокупности условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. В рамках проведения мероприятий по моделированию УБИ, наиболее часто применяются следующие методики:

Международные
- TRIKE;
- PASTA;
- STRIDE и др.

Отечественные
- Методика оценки угроз безопасности информации ФСТЭК России;
- Методика определения актуальных угроз персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

АСУ ТП в соответствии с Федеральным законом № 187 от 26.07.2017 г. относятся к объектам критической информационной инфраструктуры (ОКИИ) Российской Федерации. В целях оценки угроз информационной безопасности ОКИИ, обязательным к исполнению является методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России от 05.02.2021 г. Данная методика ориентирована на оценку антропогенных УБИ АСУ ТП, возникновение которых обусловлено действиями нарушителей.

Среди международных подходов к оценке УБИ стоит выделить методику TRIKE, которая широко используется при моделировании угроз для программного обеспечения АСУ ТП, однако данная методика может иметь применение и на аппаратном уровне промышленных систем.

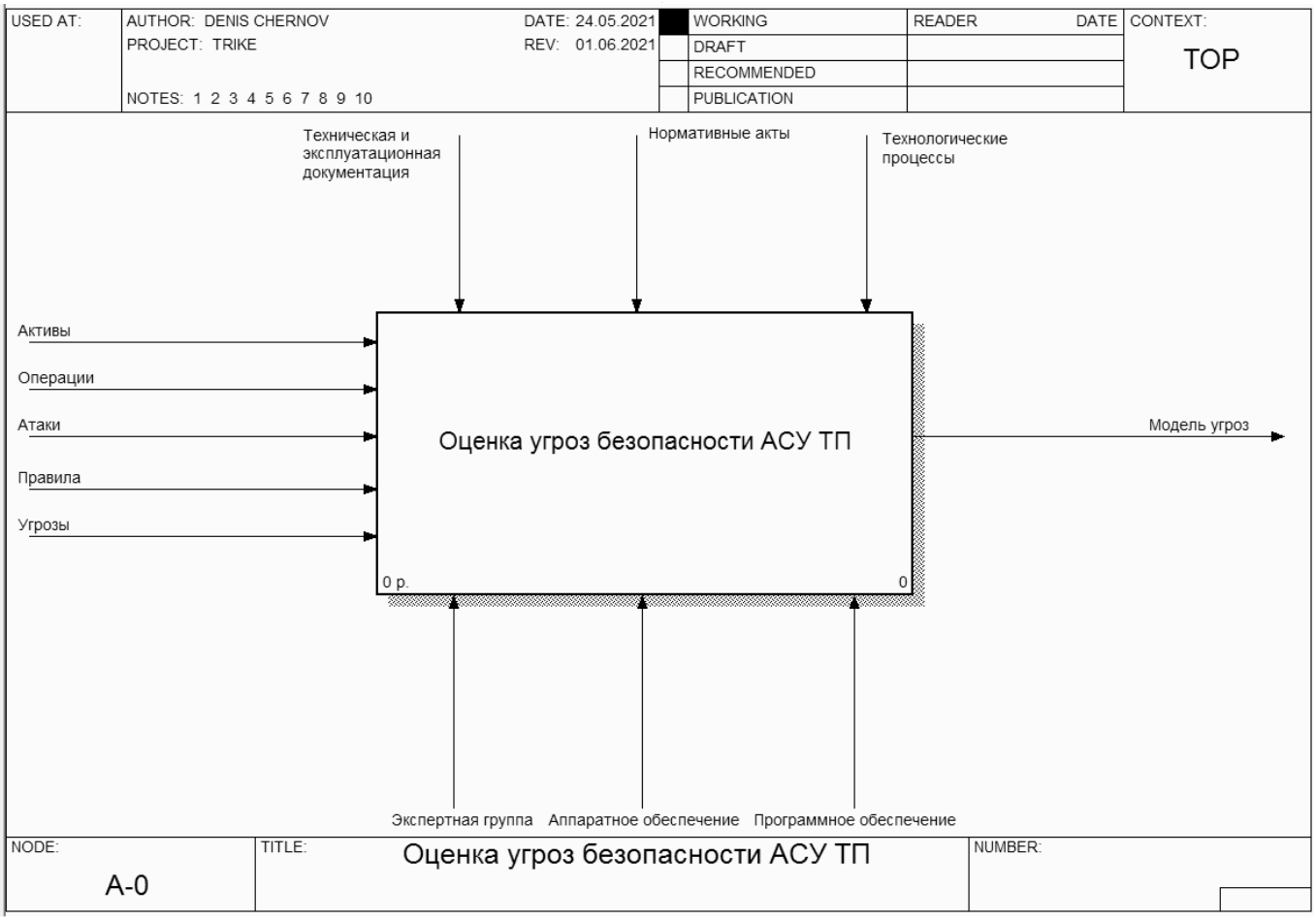


Рис. 2. IDEF0-модель методики TRIKE

В основе методики TRIKE лежит структура использования модели УБИ как инструмента управления рисками АСУ ТП, в то время как методика ФСТЭК РФ использует результаты оценки рисков (ущерба), проведенной обладателем ин-формации или оператором АСУ ТП.

В таблице 2 представлена сравнительная характеристика двух рассматриваемых методик с указанием основных критериев оценки УБИ.

По результатам анализа характеристик методик, представленных в таблице, можно сделать вывод о различающихся подходах при формировании перечней угроз АСУ ТП.

Моделирование методик оценки УБИ

В целях визуализации различий рассматриваемых методик, проведено функциональное моделирование с применением методологии IDEF0 [8,9,10]. На рисунке 1 представлена функциональная модель процесса оценки УБИ в соответствии с методикой ФСТЭК РФ.

На рис. 2 продемонстрирована функциональная модель процесса оценки УБИ в соответствии с методикой TRIKE.

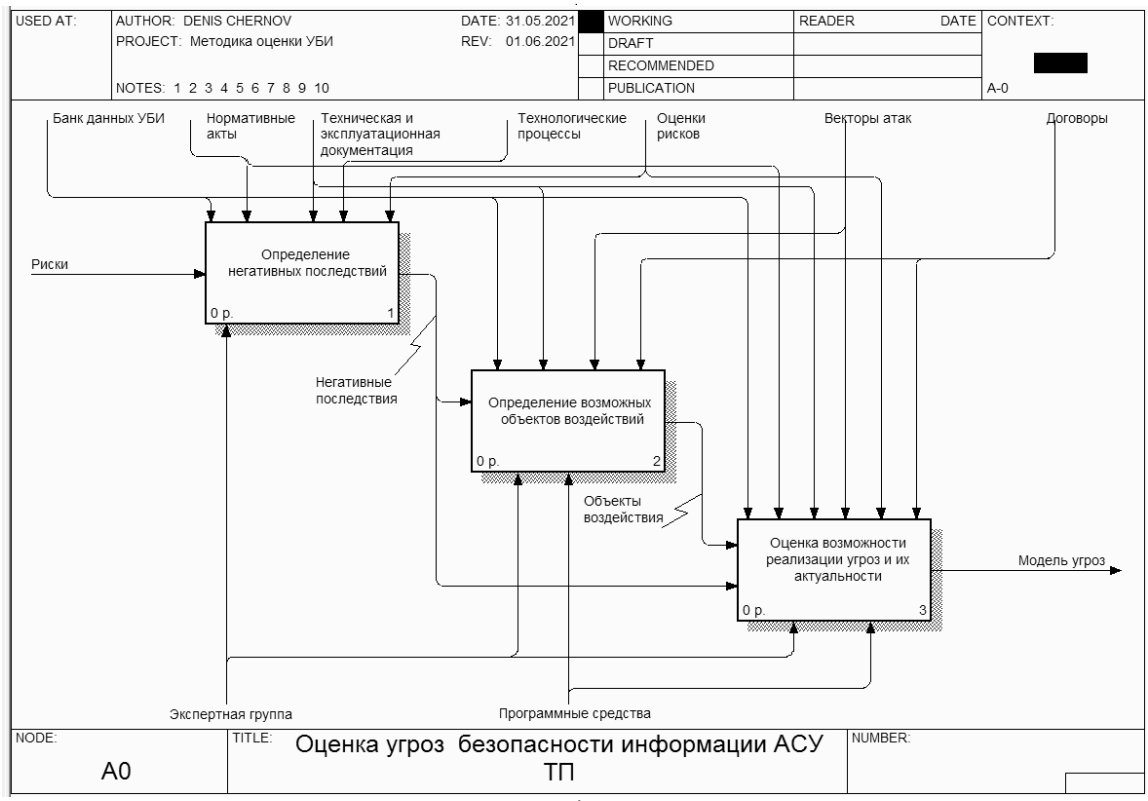
В соответствии с методикой ФСТЭК РФ, УБИ i возможна, если имеется нарушитель или иной источник угрозы $N(i)$, объект $O(i)$, на который осуществляются воздействия, способы реализации УБИ $R(i)$, а реализация угрозы может привести к негативным последствиям $P(i)$. Таким образом, УБИ характерные для АСУ ТП, будут определяться на основании (1).

$$U_i = \left[N(i); O(i); R(i); P(i)\right] \quad (1)$$

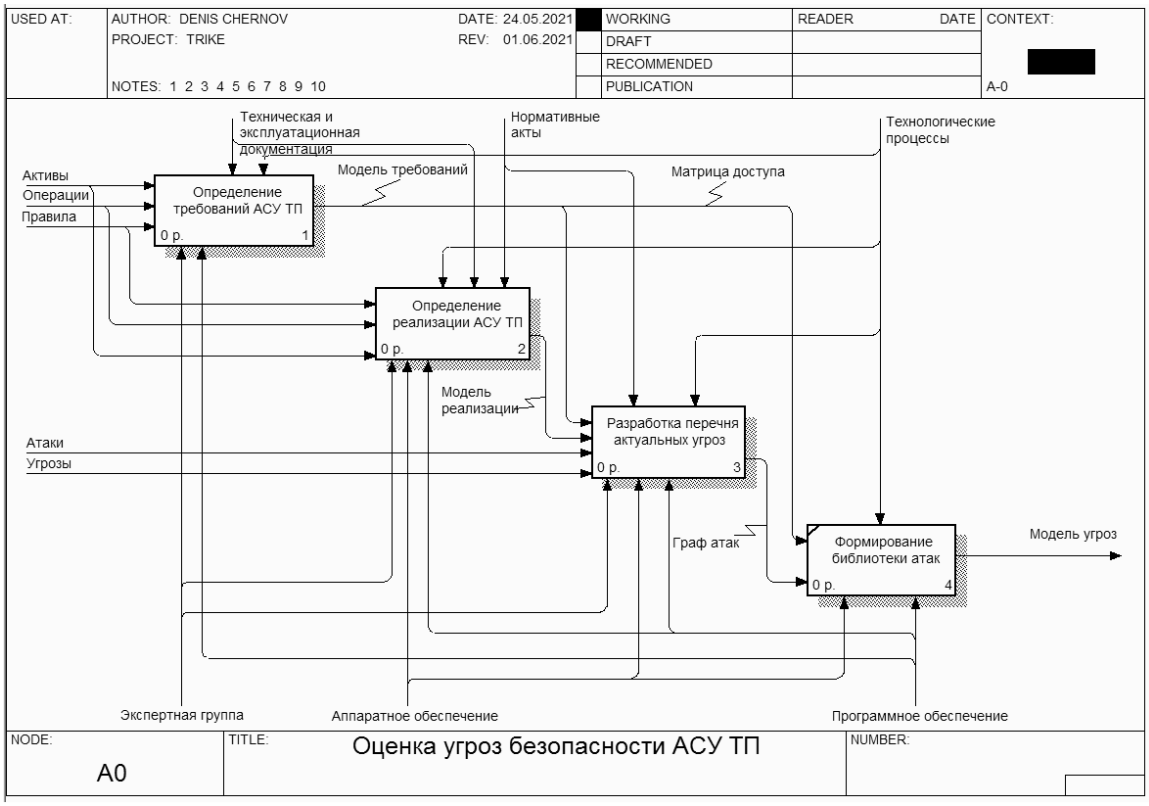
Актуальность возможных УБИ определяется наличием хотя бы одного сценария каждого способа реализации возможной УБИ в соответствии с (2).

$$U_i^s = F(i,s), \quad (2)$$

где $F(i,s) \in \{0,1\}$ — функция принадлежности для угроз, характеризующая актуальность i-й угрозы при наличии s сценариев её реализации.



а)



б)

Рис. 3. Декомпозиция функционального блока Оценка УБИ методики ФСТЭК РФ — *а*. Декомпозиция функционального блока Оценка УБИ методики TRIKE — *б*

В соответствии с результатами определения сценариев реализации угроз, функция принадлежности $F(i,k)$ принимает значения:

0 — неактуальная угроза, $s = 0$;

1 — актуальная угроза, $s \geq 1$.

Сценарий определяется для каждого нарушителя и их уровней возможностей.

Перечень УБИ, в соответствии с положениями методики TRIKE, генерируется на основе полученной «модели требований» с использованием следующего алгоритма действий: для каждой предполагаемой операции создается одна угроза категории «отказ в обслуживании». На следующем этапе набор запланированных операций инвертируется в целях формирования набора запрещенных операций. При этом создается угроза категории «повышение привилегий» для каждого из набора запрещенных операций. Затем для каждой запланированной операции генерируются угрозы «повышения привилегий» полностью и частично запрещенных операций и затем к полученному набору угроз добавляется угроза «социальной ответственности» т.е. угроза того, что субъект использует эту систему для принятия мер против другой системы. Таким образом, методикой TRIKE охватываются большинство актуальных УБИ АСУ ТП, а полученную по описанному алгоритму модель угроз безопасности информации можно формализовать в соответствии с (3).

$$U_{di} = \sum_{d=1}^{n}\left(U_d(a) + \sum_{i=1}^{3} U_{\overline{d}}(b_i)\right), \quad (3)$$

Где U_d — угрозы в отношении операций $d = \overline{1,n}$, $U_d(a)$ — функция, характеризующая угрозу категории «отказ в обслуживании» в отношении операций d, а функция $U_{\overline{d}}(b_i)$ описывает угрозы категории «повышение привилегий» $b_i, i = \overline{1,3}$, для инвертированной операции $\overline{d}$ при следующих условиях: b_1 — угроза полностью запрещенного действия, b_1 — угроза частично запрещенного действия, b_1 — угроза «социальной ответственности».

На рисунке 3 представлена декомпозиция функциональных блоков «оценка угроз безопасности информации АСУ ТП», отражающая формализованное представление подходов к моделированию угроз информационной безопасности рассматриваемых методик оценки УБИ. Данная декомпозиция визуализирует основные отличия методик, в частности, наличие в методике TRIKE библиотеки атак.

Основное отличие рассматриваемых методик заключается в том, что методика TRIKE подразумевает автоматизированное построение графа атак на АСУ ТП по завершении формирования конечного перечня УБИ, формируя библиотеки атак на основе однотипных путей графа, а методика ФСТЭК РФ позволяет использовать типовые техники, используемые для построения сценариев реализации УБИ АСУ ТП.

Исходя из вышесказанного, можно сделать вывод о том, что методика ФСТЭК РФ отражает процесс оценки УБИ, ориентируясь на оснащенность и потенциал нарушителя информационной безопасности, в то время как методика TRIKE опирается на состояние системы защиты информации системы, для которой проводится оценка УБИ и последующее моделирование угроз. Поэтому в рамках реализации унифицированного подхода к моделированию угроз информационной безопасности целесообразно применять отдельные техники, описанные в методике TRIKE, (в частности — генерация дерева атак) в рамках мероприятий по оценке УБИ в соответствии с положениями методики ФСТЭК РФ.

Заключение

В статье рассмотрены основные положения наиболее используемых методик оценки УБИ АСУ ТП в России и за рубежом. Мероприятия по оценке УБИ являются важной частью процесса моделирования угроз информационной безопасности промышленных систем. Поэтому существует задача, которая заключается в унификации подходов к оценке угроз УБИ АСУ ТП. В данной статье предлагается сравнение отечественной методики ФСТЭК РФ и международной методики TRIKE, направленное на определение общих характеристик построения перечня актуальных угроз информационной безопасности, а также различий в оценке УБИ. По результатам сравнительного анализа, автором даны предложения по расширению мероприятий по оценке УБИ АСУ ТП в рамках применения методики ФСТЭК РФ.

ЛИТЕРАТУРА

1. Национальный стандарт РФ ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения» [Электронный ресурс] // ГАРАНТ.РУ: информ. правовой портал. URL: http://base.garant.ru/ 182535 (дата обращения 03.05.2021).
2. Методический документ ФСТЭК России от 05.02.2021 г. «Методика оценки угроз безопасности ин-формации» [Электронный ресурс] // URL: https://fstec.ru/en/component/attachments/download/2919 (дата обращения 05.05.2021).
3. Хорев А.А. Угрозы безопасности информации / А.А. Хорев // Специальная техника. — 2010. № 1. — С. 50–63.

4. Доктрина информационной безопасности Российской Федерации (утв. Приказом Президента РФ от 05.12.2016 г. № 646) [Электронный ресурс] // ГАРАНТ.РУ: информ. правовой портал. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения 03.05.2021).
5. Национальный стандарт РФ ГОСТ Р ИСО МЭК 27002–2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [Электронный ресурс] // URL: http://protect.gost.ru/ v.aspx?control =8&id=176022 (дата обращения 05.05.2021).
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка), утверждена ФСТЭК России 15.02.2008 г. [Электронный ресурс] // URL: https://fstec.ru/component/attachments/download/289 (дата обращения 05.05.2021).
7. Saita Paul. Trike v.1 Methodology Document [Draft] / P. Saita, B. Larcom, M. Eddington // [Электронный ресурс] URL: https://www.octotrike. org/papers/Trike_v1_Methodology_Document-draft.pdf (дата обращения 05.05.2021).
8. Шибанов С.В. Моделирование активных правил в нотации IDEF0 / С.В. Шибанов, А.А. Скоробогатько // Труды Международного симпозиума «Надежность и качество». — 2012. — Т. 1. — С. 436–438.
9. Ананьев И.В. Области эффективного применения нотации IDEF0 для задач описания бизнес-процессов / Ананьев И.В., Серова Е.Г. // Вестник Санкт-Петербургского университета. Менеджмент. — 2008. — № 1. — С. 161–172.
10. Зимовец О.А. Представление диаграмм в нотациях DFD, IDEF0 и BPMN с помощью системно-объектных моделей «Узел-функция-объект» / Зимовец О.А., Маторин С.И. // Экономика. Информатика. — 2011. — Т. 114, № 19–1. — С. 133–144.

Журнал «Современная наука: актуальные проблемы теории и практики»

Тульский Государственный университет