УДК 519.242.7 Вестник УрФО № 2(60) / 2026, с. 32–46

Поршнев С.В., Сафиуллин Н.Т.

DOI: 10.14529/secur260204

АНАЛИЗ ОПЫТА ПРИМЕНЕНИЯ МЕТОДА ФАКТОРНОГО ЭКСПЕРИМЕНТА В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проведен анализ опыта применения метода факторного эксперимента в задачах информационной безопасности, результаты которого показали, что данный метод, несмотря на его потенциальные возможности для тестирования средств защиты и систем защиты информации не используется. Для исправления этой ситуации, по мнению авторов, целесообразно разработать научно обоснованную методику, обеспечивающую отображение семантических описаний угроз безопасности информации, уязвимостей средств и систем в количественные значения входных факторов (варьируемых показателей), а также оценку влияния данных показателей на безопасность защищаемой информационной инфраструктуры.

Ключевые слова: *метод факторного эксперимента, полный факторный эксперимент, дробный факторный эксперимент, планирование факторного эксперимента, информационная безопасность.*

Porshnev S.V., Safiullin N.T.

ANALYSIS OF THE FACTORIAL EXPERIMENT METHOD USAGE IN TASKS OF INFORMATION SECURITY

In this paper an analysis of current usage of the factorial experiment method in information security field is presented. The results show that this method has a potential usage in testing protective means and defensive systems, but currently underused. To improve its usability, it is suggested to develop a scientifically sound methodology that ensures the mapping of semantic descriptions of potential threats in information security and vulnerabilities into quantitative values of input factors (varying parameters), as well as an assessment of the influence of these factors on the safety of the protected information infrastructure.

Keywords: *factorial experiment method, full factorial experiment, fractional factorial experiment, full factorial design, information security.*

1. Введение

В современных условиях задача оценки безопасности[1] информационной инфраструктуры (совокупности объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией РФ или используемых на основании международных договоров РФ[2]), а также объектов критической информационной инфраструктуры[3] (КИИ) и различных программных приложений. (Соответственно, понятие «опасность» для объекта можно определить как реальное (существующее, действующее) или потенциально возможное состояние объекта, которое может привести к ущербу в существовании, функционировании, развитии объекта[4]).

Для решения данной задачи, сегодня, наиболее популярными оказываются подходы, основанные на методах теории оценки рисков, методов интеллектуального анализа данных, формальных методах информационной безопасности, статистическом моделировании кибератак (см., например, [1–12]).

Для оценки безопасности информационной инфраструктуры также активно используется методология «черного ящика» (ЧЯ) (англ., *Black Box*) [13], которая наиболее часто, как показали результаты информационного поиска в сети Интернет, используется для динамического тестирования средств защиты информации (СрЗИ), а также программного обеспечения (англ. *Dynamic Application Security Testing, DAST*) с целью обнаружения в них уязвимостей (проведения пентестов), которые может использовать нарушитель для проведения компьютерных атак (КА). Среди инструментов динамического тестирования безопасности, включенных в реестр отечественного программного обеспечения, отметим: *PT Application Inspector, PT BlackBox (Positive Technologies); AppChecker Cloud* (АО «НПО «Эшелон»); *SafeERP* («Газинформсервис»); *BI.ZONE* Анализ защищенности приложений (компания *BI.ZONE*); *Linx SAST* (компания *Linx*); *Solar AppScreener* (компания *Solar*); Айтуби (компания Айтуби).

Напомним, что методология ЧЯ, была разработана для построения статистических моделей сложных систем, формализованное описание структуры которых неизвестно системы (в том числе, неизвестны структура системы, механизмы и правила взаимодействия, входящих в нее подсистем, отсутствует математическая модель системы, разработанная на основе использования аналитических методов, например, вследствие отсутствия соответствующих физических моделей системы и/или адекватного математического аппарата), на основе результатов экспериментальных исследований, называемых факторным экспериментом[5] (ФЭ), проводимых в соответствие с планом факторного эксперимента (см., например, [14], где приведены ссылки на соответствующие монографии, в которых заложены теоретические основы метода ФЭ).

Однако, анализ перечисленных выше инструментов динамического тестирования показывает, что ни один из них не предоставляет пользователю функционала для планирования, проведения и анализа результатов ФЭ, на основе модели ЧЯ. С нашей точки зрения, данная ситуация, в первую очередь, обусловлена отсутствием способов отображения векторов КА, представляющих собой некоторые формальные текстовые описание в виде строк, содержащих соответствующие шифры КА, во входные выходные и факторы ЧЯ, измеряемые в количественных шкалах, а также способов обратного отображения количественных входных и выходных факторов в понятийное пространство ИБ и их интерпретации в данном пространстве.

В этой связи авторы:

Изучили опыт использования ФЭ для решения задач ИБ.

[1] В соответствие с Толковым словарем русского языка: «безопасность» (объекта) – это состояние (объекта), при котором (объекту) не угрожает опасность, имеется защита (объекта) от опасности; «опасность» – возможность, угроза чего-либо очень плохого, какого-либо несчастья; угроза – возможная опасность.

[2] Доктрина информационной безопасности РФ. Утверждена Указом Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Подпункт «з» пункта 2.

[3] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция).

[4] В действующих НПА в области ИБ также используется понятие «фактор, воздействующий на защищаемую информацию», смежное с понятием «угроза» (см. например, «Выписку из Концепции государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы Российской Федерации», утвержденной Президентом РФ 12 декабря 2014 г. № К-1274).

[5] «Фактор» (лат. factor «делающий, производящий») – причина, движущая сила какого-либо процесса, определяющая его характер или отдельные его черты.//Большая советская энциклопедия : [в 30 т.] / гл. ред. А. М. Прохоров. –3-е изд. –М. : Советская энциклопедия, 1969-1978. [Электронный ресурс]. - URL: https://bigenc.ru/c/eksperiment-509478 (дата обращения: 17.11.2024).

Провели самостоятельный анализ источников информации о КА и технологиях их реализации, в том числе:

– каталог известных уязвимостей ИБ *MITRE*[6] *CVE* (*Common Vulnerabilities and Exposures*) [15];

– базу знаний *MITRE ATT&CK* (*Adversarial Tactics, Techniques & Common Knowledge*) [16], содержащую модели реальных сценариев компьютерных атак (модели поведения злоумышленников), которая собрана на основе анализа тысяч инцидентов ИБ;

– базу знаний *MITRE D3FEND* (де-факто, базу защитных техник) [17], базу данных угроз безопасности информации БДУ ФСТЭК России [18];

– Методический документ «Методика оценки угроз безопасности информации» [19].

Отметим, что в известных работах [20–], посвященных анализу контента информации размещенной в каталоге *MITRE CVE* и базах знаний *MITRE ATT&CK, MITRE D3FEND*, с точки зрения возможности ее использования для планирования ФЭ, ранее не проводился.

Научная новизна настоящей статьи состоит в разработки модели ЧЯ, используемой далее для проведения ФЭ с целью оценки безопасности информационно-телекоммуникационных систем и средств защиты информации, в терминах *MITRE CVE, MITRE ATT&CK, MITRE D3FEND*.

2. Анализ опыта применения ПФЭ в задачах ИБ

Рассмотрим примеры задач ИБ, для решения которых использовался метод ФЭ.

1) Для оценки вероятностей угроз ИБ [26].

Здесь для некоторого анонимного предприятия Z оценивалась вероятность проникновения нарушителя в помещение, в котором находится ИС, в предположении, что на реализацию угрозы оказывают влияние следующие факторы рисков:

1. X_1 – выход из строя электронного замка;
2. X_2 – выход из строя видеокамер;
3. X_3 – инсайдер, который может сообщить нарушителю о выходе из строя электронного замка и/или видеокамер.
4. X_4 – сотрудник, который может случайно пропустить нарушителя в помещение, в котором располагается информационная система.

В связи с тем, что модель ПФЭ в этом случае состояла из 16 опытов, авторы использовали модель дробного факторного эксперимента, состоящего из 8 опытов, матрица которого представлена в таблице 1.

Таблица 1

Таблица плана факторного эксперимента

№	X_0	X_1	X_2	X_3	X_1X_2	X_1X_3	X_2X_3	X_4 $X_1X_2X_3$	*Y*
1	+1	–1	–1	–1	+1	+1	+1	–1	0
2	+1	+1	–1	–1	–1	–1	+1	+1	0,1
3	+1	–1	+1	–1	–1	+1	–1	+1	0,1
4	+1	+1	+1	–1	+1	–1	–1	–1	0,2
5	+1	–1	–1	+1	+1	–1	–1	+1	0,8
6	+1	+1	–1	+1	–1	+1	–1	–1	0,85
7	+1	–1	+1	+1	–1	–1	–1	+1	0,9
8	+1	+1	+1	+1	+1	+1	+1	+1	1,0

Входным факторам X_n, $n = \overline{1,4}$ присваивались значения ± 1 (+1 – угроза реализуется, –1 – угроза отсутствует). Значения выходного показателя Y_1, $i = \overline{1,8}$ (вероятности угроз получения доступа нарушителя к информационной системе) при сочетаниях входных факторов, указанных в таблице 1, оценивалась экспертом.

Оказалось, что функция отклика описывается следующим выражением:

$Y = 0,5 + 0,0375X_1 + 0,0625X_2 + 0,385X_3 + 0,0125X_4$,

из которого видно, что наибольшее влияние на функцию отклика оказывает фактор X_3, наименьшее фактор – X_4.

2) Для оценки угроз и рисков информационной безопасности на примере оценки вероятности внедрения внутренним нарушите-

[6] MITRE – американская некоммерческая организация, взаимодействующая с оборонными и гражданскими ведомствами США, которая разрабатывает модели, стандарты, инструменты, базы знаний в области кибербезопасности.

лем вредоносного кода [27]. Здесь для некоторого предприятия Z оценивалась вероятность реализации внедрения внутренним нарушителем вредоносного кода в предположении, что на реализацию угрозы оказывают влияние следующие факторы рисков:

1. X_1 – устаревшие антивирусные базы;

2. X_2 – отсутствие запрета на запуск исполняемых файлов от имени пользователей;

3. X_3 – возможность управления функционированием антивирусного ПО от имени пользователей;

4. X_4 – возможность установления удаленного подключения к персональному компьютеру.

Для построения модели, описывающей зависимость вероятности внедрения внутренним нарушителем вредоносного кода Y от выбранных факторов X_1, X_2, X_3, X_4. В связи с тем, что модель ПФЭ в этом случае состояла из 16 опытов, авторы использовали модель дробного факторного эксперимента, состоящего из 8 опытов, план которого представлен в таблице 2.

Таблица 2

Таблица плана ПФЭ

№	X_0	X_1	X_2	X_3	X_4 $X_1X_2X_3$	X_1X_2	X_1X_3	X_2X_3	Y
1	+1	−1	−1	−1	−1	+1	+1	+1	0
2	+1	+1	−1	−1	+1	−1	−1	+1	0,95
3	+1	−1	+1	−1	+1	−1	+1	−1	0,87
4	+1	+1	+1	−1	−1	+1	−1	−1	0,97
5	+1	−1	−1	+1	+1	+1	−1	−1	0,82
6	+1	+1	−1	+1	−1	−1	+1	−1	0,96
7	+1	−1	+1	+1	−1	−1	−1	+1	1,0
8	+1	+1	+1	+1	+1	+1	+1	+1	0,8

Входным факторам X_n, $n=\overline{1,4}$ присваивались значения ± 1 (+1 – угроза реализуется, −1 – угроза отсутствует). Значения выходного показателя Y_i, $i=\overline{1,8}$ (вероятности угроз получения доступа нарушителя к информационной системе) при сочетаниях входных факторов, указанных в таблице 2, оценивалась экспертом.

Оказалось, что функция отклика описывается следующим выражением:

$$Y = 0.82 + 0,15X_1 + 0,14X_2 + 0,12X_3 + 0,09X_4 - 0,13X_1X_2 - \\ - 0,12X_1X_3 - 0,9X_2X_3,$$

из которого видно, что наибольшее влияние на функцию отклика оказывают факторы X_1, X_2, наименьшее – фактор X_4.

3) Для оценки факторов, влияющих на реализацию угроз и рисков информационной безопасности [28]. Здесь была использована модель угроз безопасности информации, обрабатываемой в системе электронного документооборота, составленная в соответствии с требованиями Методического документа «Методика оценки угроз безопасности информации» (утв. ФСТЭК от 5 февраля 2021 г.) [19] и на основании банка угроз [18]. Оценку рисков выполняли для группы угроз, реализуемых в государственной организации внутренним нарушителем с низким потенциалом, что приводит к нарушению конфиденциальности, целостности и доступности информации [18]:

– УБИ.074 – угроза несанкционированного доступа к аутентификационной информации;

– УБИ.086 – угроза несанкционированного изменения аутентификационной информации;

– УБИ.088 – угроза несанкционированного копирования защищаемой информации;

– УБИ.152 – угроза удаления аутентификационной информации;

– УБИ.167 – угроза заражения компьютера при посещении неблагонадёжных сайтов;

–УБИ.168 – угроза «кражи» учётной записи доступа к сетевым сервисам;

– УБИ.172 – угроза распространения «почтовых червей»;

– УБИ.191 – угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

В качестве причин реализации угрозы несанкционированного доступа к аутентификационной информации (УБИ.074 [16]) были рассмотрены следующие факторы:

1) X_1 – небрежность действий персонала в информационном измерении;

2) X_2 – использование устаревших антивирусных баз;

3) X_3 – отсутствие запрета на запуск исполняемых файлов от имени пользователей;

4) X_4 – возможность управления функционированием антивирусного программного обеспечения от имени пользователей.

Матрица плана проведенного 2^3-дробного факторного эксперимента представлена в таблице 3.

Вероятность реализации угроз для каждого сценария $\left(Y_{i,j}\right)$ оценивалась экспертным методом (метод непосредственного оценивания) по шкале от 0 до 1. Объектам экспертизы (каждому сценарию) каждым экспертом присваивались баллы, при этом наиболее значимому объекту (сценарию) присваивалось наибольшее количество баллов в соответствие с выбранной шкалой оценок. Вероятность реализации угроз для каждого сценария $\left(Y_i\right)$ оценивалась как среднее арифметическое значение оценок сценариев каждым из четырех экспертов. Результаты оценки вероятностей реализации угроз методом экспертных оценок представлены в табл. 4.

На основании результатов оценки вероятностей реализации угрозы (табл. 4) для восьми планов проведения 4-х факторных

Таблица 3

Таблица плана факторного эксперимента

№	X_0	X_1	X_2	X_3	X_4	X_1X_2	X_1X_3	X_2X_3	Y
1	+1	−1	−1	−1	−1	+1	+1	+1	Y_1
2	+1	+1	−1	−1	+1	−1	−1	+1	Y_2
3	+1	−1	+1	−1	+1	−1	+1	−1	Y_3
4	+1	+1	+1	−1	−1	+1	−1	−1	Y_4
5	+1	−1	−1	+1	+1	+1	−1	−1	Y_5
6	+1	+1	−1	+1	−1	−1	+1	−1	Y_6
7	+1	−1	+1	+1	−1	−1	−1	+1	Y_7
8	+1	+1	+1	+1	+1	+1	+1	+1	Y_8

Таблица 4

Результаты оценки вероятностей реализации угроз методом экспертных оценок

№	Ранги $R_{i,j}$, присвоенные экспертами				$\sum_{i=1}^{2^3} R_{i,j}$	Y_j
1	0,30	0,30	0,30	0,40	1,30	0,33
2	0,50	0,50	0,50	0,60	2,10	0,53
3	0,40	0,60	0,50	0,50	2,00	0,50
4	0,50	0,70	0,60	0,70	2,50	0,63
5	0,80	0,70	0,80	0,60	2,90	0,73
6	0,70	0,80	0,80	0,80	3,10	0,78
7	0,85	1,00	0,90	0,70	3,45	0,86
8	1,00	1,00	0,95	1,00	3,95	0,99

экспериментов, представленных в табл. 3, получена следующая функции отклика:

$$Y = 0,669 + 0,064X_1 + 0,076X_2 + 0,171X_3 + 0,001X_1X_2 - 0,019X_1X_3 + 0,009X_2X_3.$$

Авторы интерпретировали найденное выражение для функции отклика следующим образом: значение $b_0 = 0,669 > 0,5$ свидетельствует об актуальности рассматриваемой угрозы и значимости влияния каждого из четырех рассмотренных факторов на реализацию угрозы информационной безопасности. Наибольший вклад в реализацию угрозы информационной безопасности вносит влияние фактор X_3 – отсутствие запрета на запуск исполняемых файлов от имени пользователей, который также усиливает и усиливает негативное действие фактора X_2 – использование устаревших антивирусных баз, а также уменьшает влияние X_1 – (небрежность действий персонала в информационном измерении). Наименьшее влияние на вероятность реализации угрозы фактор X_4 – возможность управления функционированием антивирусного программного обеспечения от имени пользователей.

4) Для разработки методики оценки эффективности системы менеджмента информационной безопасности (СМИБ) по времени реакции системы на инциденты ИБ [28]. В качестве интегрального показателя эффективности системы менеджмента информационной безопасности предложено использовать время реакции СМИБ на инциденты ИБ, вычисляемое по формуле:

$$T_{\text{рсИБ}} = \sum_{i=1}^{k} \left(T_{\text{обнИБ}_i} + T_{\text{блокИБ}_i} + T_{\text{регИБ}_i} + T_{\text{оповИБ}_i} \right),$$

где k – количество атрибутов, подлежащих измерению; $T_{\text{рсИБ}}$ – время реакции СМИБ на инцидент ИБ; $T_{\text{обнИБ}_i}$ – время обнаружения инцидента ИБ; $T_{\text{блокИБ}_i}$ – время блокирования несанкционированных действий по нарушению ИБ; $T_{\text{регИБ}_i}$ – время регистрации события, связанного с инцидентом ИБ; $T_{\text{оповИБ}_i}$ – время оповещения персонала службы ИБ о выявленном инциденте ИБ.

Для расчета показателя автор рекомендовал разделить меры и средства управления и контроля для выполнения проверок на группы по времени реагирования на инцидент ИБ, и использовать следующие виды группирования:

– немедленный контроль (время реакции – несколько минут ($T_{\text{рсИБ}} \le 10$ мин));

– суточный контроль (время реакции – в течение суток ($T_{\text{рсИБ}} \le 24$ ч));

– контроль изменения политик ИБ (время реакции – в течение нескольких суток ($T_{\text{рсИБ}} \le 10$ сут)).

В связи с тем, что для исследованных мер и средств управления и контроля СМИБ функция отклика (аналитической модели), описывающая показатель эффективности СМИБ, получить ее аналитического описания не удалось, автор, предложил использовать метод ПФЭ или ДФЭ, однако, не привел ни каких-либо наборов варьируемых факторов, ни диапазонов их изменений.

Предложенная в [28] методика расчета показателя эффективности СМИБ реализуется выполнением следующей последовательности действий.

1. Выбор необходимого количества атрибутов k и требуемого числа измерений N.

2. Выбор, исходя из априорных данных и экспертных оценок, модели, описывающей, описывающей функциональную зависимость времени реакции СМИБ на инциденты ИБ $T_{\text{рсИБ}}$.

3. Определение интервалов варьирования входных факторов с учетом особенностей СМИБ организации.

4. Выбор ПФЭ (для случая $k \le 3$) или ДФЭ (для случая $k > 3$).

5. Составление матрицы плана ФЭ, удовлетворяющей требованиям D-оптимального плана, и определение, в соответствие с выбранным планом, правила вычисления коэффициентов регрессии b_j.

6. Проведение измерения значений выходного показателя для значений входных факторов, указанных в матрице плана ФЭ.

7. Расчет по результатам измерений коэффициентов регрессии b_j.

8. Проверка статистической значимости коэффициентов регрессии b_j, а также адекватности построенной математической модели.

При этом, однако, автор не привел ни одного конкретного примера использования предложенной методики.

Таким образом, результаты анализа опыта использования метода факторного эксперимента в ИБ позволяют сделать следующие выводы.

1. Метод факторного эксперимента использовался ранее для:

1) оценки вероятности проникновения нарушителя в помещение, в котором находится информационная система;

2) вероятностей угроз и рисков ИБ на примере оценки вероятности внедрения

внутренним нарушителем вредоносного кода;

3) ранжирования факторов, влияющих на реализацию угроз ИБ;

4) разработки методики оценки эффективности СМИБ.

2. В качестве входных варьируемых факторов в данных экспериментах использовались следующие группы факторов:

1) выход из строя электронного замка (X_1); выход из строя видеокамер (X_2); инсайдер, который может сообщить нарушителю о выходе из строя электронного замка и/или видеокамеру (X_3); сотрудник, который может случайно пропустить нарушителя в помещение, в котором располагается информационная система (X_4);

2) устаревшие антивирусные базы (X_1); отсутствие запрета на запуск исполняемых файлов от имени пользователей (X_2); возможность управления функционированием антивирусного ПО от имени пользователей (X_3); возможность установления удаленного подключения к персональному компьютеру (X_4);

3) небрежность действий персонала в информационном измерении (X_1); использование устаревших антивирусных баз (X_2); отсутствие запрета на запуск исполняемых файлов от имени пользователей (X_3); возможность управления функционированием антивирусного программного обеспечения от имени пользователей (X_4);

4) входные варьируемые факторы не указаны.

3. Значения входных варьируемых факторов измерялись по дихотомической шкале (+1 – данная угроза безопасности ИБ присутствует, –1 – данная угроза безопасности информации отсутствует).

4. Значения выходного показателя, характеризующего состояния ИБ изучаемой системы, определялись на основе экспертных оценок, но не результатов их измерений реальных факторных экспериментах.

5. Публикаций с обсуждением результатов применения методов ПФЭ и ДФЭ для тестирования средств защиты и систем защиты информации обнаружить не удалось.

3. Модель «черного ящика» в терминах матриц MITRE ATT&CK и MITRE D3FEND

Предваряя обсуждение модели ЧЯ в терминах матриц MITRE ATT&CK и MITRE D3FEND, рассмотрим классическую постановку задачи, для решения которой используется модель ЧЯ. Имеется система, рассматриваемая как некоторое изолированное целое, содержащее совокупность процессов и средств их реализации, представляющая собой ЧЯ, на который воздействует некоторое конечное множество независящих друг от друга контролируемых (задаваемых) воздействий $\{x_n\}$, $n=\overline{1,N}$ – входных факторов, а также некоторое конечное множество контролируемых неизменяемых факторов (условия, среда функционирования и т.п.) $\{c_k\}$, $k=\overline{1,K}$ и некоторое конечное множество неконтролируемых или контролируемых, но неуправляемых факторов (случайные или неидентифицируемые воздействия, изменения, «дрейф» параметров и т.п.) $\{u_l\}$, $l=\overline{1,L}$. При этом состояние ЧЯ, как полагают, априори, можно описать некоторым конечным множеством, измеряемых независимых друг от друга показателей, $\{Y_m\}$, $m=\overline{1,M}$, называемых откликами (рис. 1).

В наиболее общей математической форме сформулированные выше исходные предположения (аксиомы) относительно факторов $\overline{X}$, $\overline{C}$ и $\overline{U}$, определяющих значения откликов «черного ящика» $\overline{Y}$, записываются в следующем виде:

$$\overline{Y}=\overline{F}\left(\overline{X},\overline{C},\overline{U}\right), \qquad (1)$$

где: $\overline{Y}=(y_1,y_2,\ldots,y_M)$ – вектор размерности M, содержащий значения выходных оцениваемых (измеряемых) показателей, характеризующих состояние «черного ящика, которые выбираются, исходя из целевых аспектов проводимого экспериментального исследования;

$\overline{X}=(x_1,x_2,\ldots,x_N)$ – вектор размерности N, содержащий значения варьируемых факторов;

$\overline{C}=(c_1,c_2,\ldots,c_K)$ – вектор размерности K, содержащий значения контролируемых, но неизменяемых факторов исследования;

$\overline{U}=(u_1,u_2,\ldots,u_L)$ – вектор размерности L, содержащий значения неконтролируемых или контролируемых, но не управляемых (случайных, неидентифицируемых) факторов;

$\overline{F}$ – в общем виде некоторая векторфункция (в наиболее общем случае, функционал), ставящая в соответствие векторам $\overline{X},\overline{C},\overline{U}$, вектор $\overline{Y}$, содержащий значения (выходных) показателей состояния «черного ящика».

Говорят, что множество векторов $\overline{F}$ образует пространство выходных показателей.

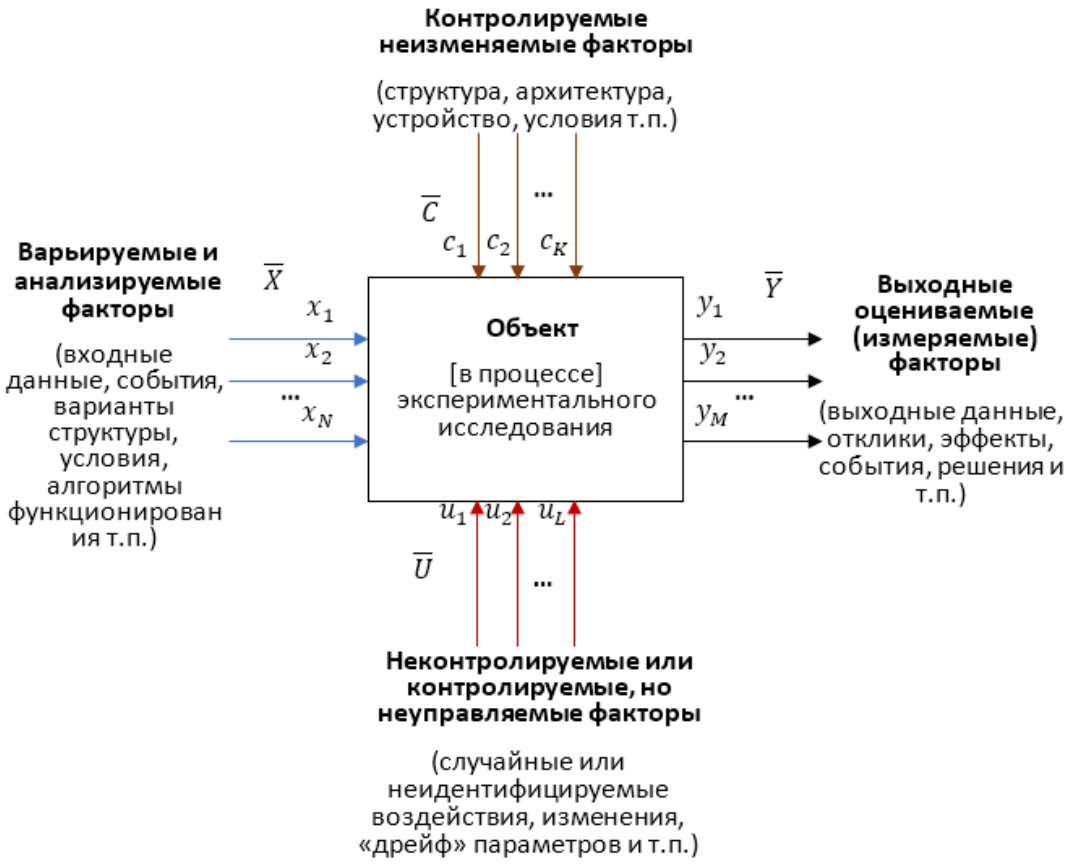

Рис. 1. Модель объекта в процессе экспериментального исследования в идеологии «черного ящика

Отметим главное требование к варьируемым и контролируемым факторам – они должны быть принципиально наблюдаемыми (измеряемыми, фиксируемыми), значимыми и существенными (оказывающими влияние на состояние объекта исследования), а также независимыми друг от друга (эквивалентно, некоррелированными друг с другом). При этом природа факторов и соответственно шкалы их измерения могут быть совершенно различными: количественными, качественными, дихотомическими, структурно-образными и т.д. (Например, при тестировании СЗИ могут определяться или вычисляться вероятности обнаружения атак, т.е. количественные факторы; при исследованиях защищенности – наличие и идентификация уязвимостей, т.е. дихотомически-назывные факторы, и т.д.). В этой связи на первом этапе планирования экспериментов все факторы и выходные показатели должны быть отображены в соответствующие цифровые значения. Относительно неконтролируемых факторов принимается постулат о том, что в ходе проводимых экспериментов их значения остаются постоянными.

Цель проведения экспериментального исследования состоит в идентификации неизвестной функции (функционала) $\overline{F}$ в (1) на основе использования задаваемых количественных значений входных факторов $\left(\overline{X}\right)$, известных количественных значений контролируемых, но неизменяемых факторов $\left(\overline{C}\right)$, неконтролируемых или контролируемых, но не управляемых факторов $\left(\overline{U}\right)$ и измеренных количественных значений отклика «черного ящика» $\overline{Y}$.

Таким образом, что основная проблема подготовки ФЭ состоит в выборе входных факторов (внешних воздействий) и выходных показателей, характеризующих состояние защищаемой информационной системы, с целью отображения решаемой задачи ИБ в пространство «классической» модели ЧЯ. Для ее решения был проведен анализ известных разработок в области ИБ, реализованных организацией MITRE, в том числе: каталог известных уязвимостей ИБ CVE [15], базу знаний ATT&CK [16], содержащую модели реальных сценариев компьютерных атак (модели поведения злоумышленников), которая собрана на основе анализа тысяч инцидентов ИБ, и

базу знаний D3FEND (да-факто, базу защитных техник, используемых для отражения КА) [17]. Отметим, что необходимость сопоставления моделей противодействия КА и конкретных мер защиты, которые должен применять специалист по ИБ, была осознана в процессе создания базы знаний MITRE D3FEND, о чем впервые было заявлено в [30]. Здесь авторы привели таблицу, в которой были указаны ключевые аспекты сопоставления моделей противодействия КА и мер защиты, представленную на рис. 2, из которого видно, что ключевые аспекты сопоставления моделей противодействия КА и мер защиты, опирающихся на семантику IDEF-моделей, аналогичны элементам модели «черного ящика», представленной на рис. 1.3.1, используемой в ФЭ.

Действительно, входные воздействия в

TABLE I
TECHNIQUE ELICITATION QUESTIONS

How does the technology work?	Activity model element
What are the data inputs?	Activity Input
What are the data outputs?	Activity Output
When does the analysis occur?	Activity Control
What are the analytical algorithms?	Activity Mechanism
How does it work at scale?	Activity Mechanism
How can it be circumvented?	Activity Mechanism

Рис. 2. Таблица вопросов по определению используемых методик

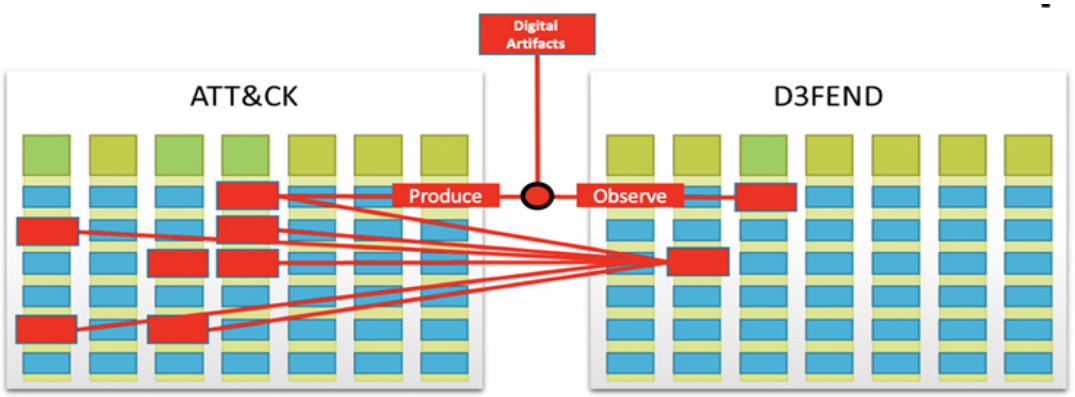

Рис. 3. Соответствие баз знаний MITRE ATT&CK и MITRE D3FEND через концепцию цифровых артефактов

модели «черного ящика» соответствуют Activity Input, выходные данные – Activity Output, контролируемые условия – Activity Control, механизмы/алгоритмы – Activity Mechanism. Однако, решение обсуждаемой задачи, как и задачи (1) (см. рис. 1) «в лоб» оказывается невозможным из-за их высоких размерностей и, как следствие, высоких временных затрат, поэтому обсуждаемая модель была декомпозирована в виде онтологии цифровых артефактов.

Для концептуального моделирования защитных техник в базу знаний MITRE D3FEND была введен новая ключевая конструкция, названная цифровым **артефактом** (Digital Artifact), а в систему их представления – онтология D3FEND DAO. В соответствие с [30], цифровой артефакт – это такой цифровой объект системы, с которым взаимодействуют атакующая систему и защищающая систем стороны, изменяя его состояние. При этом атакующая сторона создает (применяет) факторы (в терминах факторного эксперимента – варьируемые показатели) с целью изменения состояния данного цифрового артефакта (в терминах факторного эксперимента – выходные показатели), а защищающая сторона активно наблюдает за состоянием цифрового артефакта (в терминах факторного эксперимента – измеряет значения его выходных показателей) и реагирует на внешние факторы с целью обеспечения защиты (неизменяемости) цифрового артефакта или возвращения его состояния в исходное. Описанный механизм обеспечил однозначное соответствие между сценариями КА, находящихся в базе знаний MITRE ATT&CK (вход цифрового артефакта), и методик защит, находящихся в базе

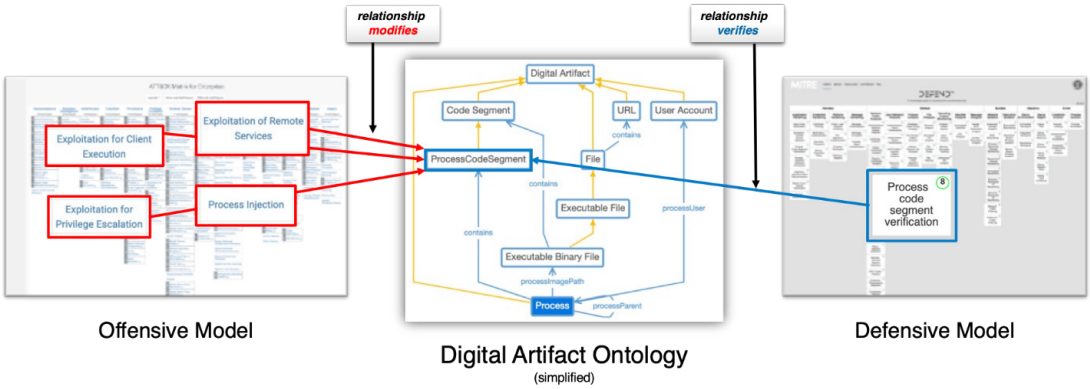

Рис. 4. Связь матриц знаний MITRE ATT&CK и MITRE D3FEND через онтологию цифровых артефактов D3FEND DAO [31]

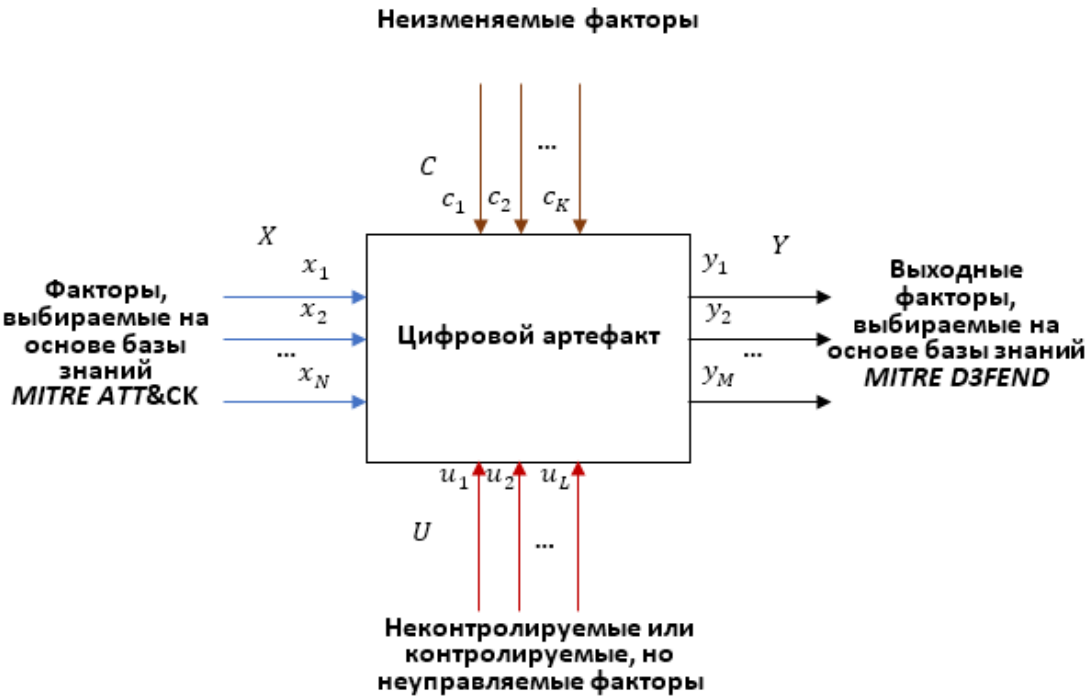

Рис. 5. Модель ЧЯ в терминах матриц MITRE ATT&CK и MITRE D3FEND

знаний MITRE D3FEND (выход цифрового артефакта) (см. рис. 3).

Отметим, что в исходной версии онтологии D3FEND DAO, артефакт в большей степени рассматривался как некоторый цифровой след, который анализировали специалисты в области ИБ, то есть, де-факто, он использовался для расследования инцидентов ИБ, но не для решения задачи противодействия атакам на ранних этапах защиты системы, либо при разработке средств защиты информации. В этой связи далее входы цифровых артефактов были связаны с базой знаний MITRE ATT&CK не только через эффект «создания» или «реализации», но и через любые другие способы воздействия на них, аналогично, независимым факторам в модели ЧЯ. При этом, принцип исключительного «наблюдения» факторов на выходе цифровых артефактов был заменен принципом «множества отношений», привязанных к защитным техникам или средствам защиты (см. пример на рис. 3).

Принимая во внимание приведенное выше определение цифрового артефакта, а также рис. 1, 3, можно предложить следующий прототип модели «черного ящика» в терминах матриц MITRE ATT&CK и MITRE D3FEND (рис. 3).

Однако для практического использования предложенного прототипа модели «черного ящика» в терминах базы знаний MITRE ATT&CK и MITRE D3FEND требуется, в свою очередь, решить следующие задачи.

1) Задачу отображения вербального опи-

сания факторов, используемых в базах знаний MITRE ATT&CK и MITRE D3FEND, в измеряемые количественные значения входных и выходных факторов, наличие которых является необходимым условием построения ПФЭ и его реализации на практике.

2) Задачу, связанную с отсутствием в онтологии цифровых артефактов D3FEND DAO определения понятия «неизменяемые факторы». (По определению цифрового артефакта, для того чтобы объект представлял собой артефакт, нужно иметь возможность наблюдения изменений его состояния, однако, любые неизменяемые факторы находятся за рамками этого термина.

3) Задачу, связанную с отсутствием в базе знаний MITRE D3FEND, как таковых, отдельных неконтролируемых (или неуправляемых) факторов, поскольку входные факторы в момент проведения КА (но не ее тестирования или моделирования) становятся неуправляемыми, так как они зависят от атакующей стороны, но не зависят от стороны защиты. (Таким образом, следует считать, что-либо известны все входные факторы цифрового артефакта, либо существуют неизвестные неконтролируемые факторы, не включенные в базу знаний MITRE D3FEND.)

Обсуждение подходов, обеспечивающих решение перечисленных выше задач, является предметом последующих публикаций.

Заключение

Результаты анализа опыта использования метода ФЭ в ИБ позволяют сделать следующие выводы.

Метод ФЭ использовался для:

1) оценки вероятности проникновения нарушителя в помещение, в котором находится информационная система;

2) вероятностей угроз и рисков ИБ на примере оценки вероятности внедрения внутренним нарушителем вредоносного кода;

3) ранжирования факторов, влияющих на реализацию угроз ИБ;

4) разработки методики оценки эффективности СМИБ.

Публикаций с обсуждением результатов применения методов ПФЭ и ДФЭ для тестирования средств защиты и систем безопасности информационной инфраструктуры обнаружить не удалось.

Обосновано, что основная проблема, препятствующая широкому использованию метода ФЭ для тестирования средств защиты и систем безопасности информационной инфраструктуры, состоит в отсутствии научно обоснованных методик отображения семантических описаний угроз безопасности информации, уязвимостей средств и систем в перечни входных варьируемых факторов, значения которых должны измеряться в количественных шкалах, а также выбора количественных показателей, характеризующих состояние ИБ защищаемой информационной системы.

На первом этапе решения данной проблемы проведен анализ известных разработок в области ИБ, реализованных организацией MITRE, в том числе: MITRE CVE, MITRE ATT&CK, D3FEND, построена модель ЧЯ в терминах матриц MITRE ATT&CK и MITRE D3FEND и определены задачи, требующих решения на последующих этапах исследования.

Литература

1. Файзулаев Д.Ф., Морозов Б.Б. Методы и средства анализа рисков информационной безопасности предприятия// Д.Ф. Файзулаев, Б.Б. Морозов/ Безопасность информационных технологий, 2017. № 3. –С. 69–73. DOI: http://dx.doi.org/10.26583/bit.2017.3.09

2. Васильев В.И., Вульфин А.М., Гузаиров М.Б. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт//В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров/ Информационные технологии, 2018. Т. 24. Вып. 4 –С. 266–273. DOI: 10.17587/it.24.266-273

3. Васильев В.И., и др. Оценка рисков кибербезопасности АСУ ТП промышленных объектов, на основе вложенных нечетких когнитивных карт//В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, В.М. Картак, Л.Р. Черняховская/ Информационные технологии, 2020. Т.26. Вып. 4. –С. 213–221. DOI: 10.17587/it.26.213-221

4. Вульфин А.М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных// А.М. Вульфин/Системная инженерия и информационные технологии, 2023. Т. 5, № 4 (13). С. 50–76. DOI: 10.54708/2658-5014-SIIT-2023-no3-p50

5. Васильев В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции)//В.И. Васильев, А.Д. Ки-

риллова, С.Н. Кухарев /Вестник УрФО. Безопасность в информационной сфере, 2018. Т. 30. Вып. 4. –С. 66–74. DOI: 10.14529/secur180410

6. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC//В.И. Васильев, А.Д. Кириллова, А.М. Вульфин/ Вопросы кибербезопасности, 2021. Т. 42. Вып. 2. С. 2–16. DOI: 10.21681/2311-3456-2021-2-2-16

7. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт//В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, А.Д. Кириллова/ Информационные технологии, 2018. Т. 24. Вып. 10. –С. 657-664. DOI: 10.17587/it.24.657-664

8. Аникин И.В. Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики//И.В. Аникин/ Системная инженерия и информационные технологии, 2023. Т. 5, Вып. 3. № 12. –С. 93–113. DOI 10.54708/2658-5014-SIIT-2023-no3-p93

9. Макаренко С.И. Критерии и показатели оценки качества тестирования на проникновение//С.И. Макаренко/Вопросы кибербезопасности, 2021. № 3(43). –С. 43–57. DOI:10.21681/2311-3456-2021-3-43-57

10. Смирнов С.И., Еремеев М.А., Магомедов Ш.Г., Изергин Д.А. Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке// С.И. Смирнов, М.А. Еремеев, Ш.Г. Магомедов, Д.А. Изергин /Russian Technological Journal, 2024. Т. 12. Вып. 3. –С. 25–36. DOI: https://doi.org/10.32362/2500-316X-2024-12-3-25-36

11. Макаренко С. И., Смирнов Г. Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры//С. И. Макаренко, Г. Е. Смирнов/ Вопросы кибербезопасности. 2021. № 6. (46). –С. 12–25. DOI:10.21681/2311-3456-2021-6-12-25

12. Котенко И.В. и др. Технологии больших данных для корреляции событий безопасности на основе учета типов связей//И.В. Котенко, А.В. Федорченко, И.Б. Саенко, А.Г. Кушнеревич А.Г./ Вопросы кибербезопасности,Ю 2017. №5 (24). –С. 2–16. DOI: 10.21681/2311-3456-2017-5-2-16

13. Организация системы сетевого мониторинга и оценки состояния информационной безопасности объекта / А.Л. Марухленко, К.Д. Селезнёв, М.О. Таныгин, Л.О. Марухленко // Известия Юго-Западного государственного университета, 2019. Т. 23. № 1. –С. 118–129. DOI: 10.21869/2223-1560-2019-23-1118-129.

14. Кобзарь А.И. Прикладная математическая статистика. Для инженеров и научных работников. –2-е изд., испр. –М.: ФИЗМАТЛИТ, 2012. –816 с.

15. URL: https://CVEform.mitre.org (Дата обращения: 22.12.2025).

16. URL: https://attack.mitre.org/ (Дата обращения: 22.12.2025).

17. URL: https://d3fend.mitre.org/ (Дата обращения: 22.12.2025.

18. Банк данных угроз безопасности информации// URL: https://bdu.fstec.ru/threat (Дата обращения: 22.12.2025).

19. Методический документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК 05.02.2021 г.)// URL: https://www.consultant.ru/document/cons_doc_LAW_378330/ (Дата обращения: 22.12.2025).

20. Kocaman Yu., Gönen S., Barişkan M.A., Karacayilmaz G., Yilmaz E.N. A Novel approach to continuous CVE analysis on enterprise operating systems for vulnerability assessment. International journal of information technology (Singapore), 2022. Vol. 14. № 3. P. 1433–1443.

21. Aghaei E, Al-Shaer E, Shadid W, Niu X. Automated cve analysis for threat prioritization and impact prediction. 2023. arXiv preprint arXiv:2309.03040. DOI: https://doi.org/10.48550/arXiv.2309.03040

22. Manjunatha A, Kota K, Babu AS, et al. Cve severity prediction from vulnerability description-a deep learning approach. Procedia Comput Sci, 2024; 235:3105–17. DOI: 10.1016/j.procs.2024.04.294

23. Sonmeza F. O., C. Hankina, Malacariab P. Dynamics: An Automatic Attack Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases. Preprint submitted to Computers and Security September 26, 2022. 22 p. URL: https://www.researchgate.net/publication/364096733_Attack_Dynamics_An_Automatic_Attack_Graph_Generation_Framework_Based_on_System_Topology_CAPEC_CWE_and_CVE_Database

24. Тулинов И.С., Губсков Ю.А., Громов Ю.Ю., Шатских В.В. Формирование базы данных уязвимостей программного обеспечения для оперативной нейтрализации угроз// И.С. Тулинов, Ю.А. Губсков, Ю.Ю. Громов Ю.Ю., В.В. Шатских/ Промышленные АСУ и контроллеры, 2018, № 3. – С. 26–30.

25. Paiva R. Cernambi Virgem Ecológico (CVE), un nuevo caucho de extracción natural con calidad y

directo de la selva amazónica a la industria del calzadohttps. DOI://doi.org/10.4067/S0718-07642021000600101

26. Белкин С.А., Белов В.М., Пивкин Е.Н. Применение факторного планирования эксперимента для оценки вероятностей угроз информационной безопасности// Ползуновский вестник, 2014. № 2. – С. 232–234.

27. Плетнев П. В., Белов В. М., Зубков Е. В., Крыжановская О. А. К вопросу об определении угроз и рисков информационной безопасности с использованием сценарного подхода, и факторного планирования эксперимента// Вестник СибГУТИ. 2016. № 4. – С. 12–18.

28. Маркелова Е.Б., Троеглазова А.В. Оценка факторов, оказывающих влияние на реализацию угроз информационной безопасности// ИНТЕРЭКСПО ГЕО-СИБИРЬ, 2023. Т. 6. № 1. – С. 165–170.

29. Шаго Ф.Н. Методика оценки эффективности системы менеджмента информационной безопасности (СМИБ) по времени реакции системы на инциденты ИБ//Научно-технический вестник информационных технологий, механики и оптики (Scientific and Technical Journal of Information Technologies, Mechanics and Optics), 2014. № 4 (92). – С. 115–123.

30. URL://www.anti-malware.ru/files/27-04-2023/28_s.jpg (Дата обращения: 22.12.2025).

31. URL: https://d3fend.mitre.org/technique/d3f:HostReboot/ (Дата обращения: 21.12.2025).

References

1. Fajzulaev D.F., Morozov B.B. Metody i sredstva analiza riskov informacionnoj bezopasnosti predpriyatiya// D.F. Fajzulaev, B.B. Morozov/ Bezopasnost' informacionnyh tekhnologij, 2017. № 3. –S. 67–73. DOI: http://dx.doi.org/10.26583/bit.2017.3.09

2. Vasil'ev V.I., Vul'fin A.M., Guzairov M.B. Ocenka riskov informacionnoj bezopasnosti s ispol'zovaniem nechetkih produkcionnyh kognitivnyh kart//V.I. Vasil'ev, A.M. Vul'fin, M.B. Guzairov/ Informacionnye tekhnologii, 2018. T. 24. Vyp. 4 –S. 266–273. DOI: 10.17587/it.24.266-273

3. Vasil'ev V.I., i dr. Ocenka riskov kiberbezopasnosti ASU TP promyshlennyh ob"ektov na osnove vlozhennyh nechetkih kognitivnyh kart//V.I. Vasil'ev, A.M. Vul'fin, M.B. Guzairov, V.M. Kartak, L.R. CHernyahovskaya/ Informacionnye tekhnologii, 2020. T.26. Vyp. 4. –S. 213–221. DOI: 10.17587/it.26.213–221

4. Vul'fin A.M. Modeli i metody kompleksnoj ocenki riskov bezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury na osnove intellektual'nogo analiza dannyh// A.M. Vul'fin/Sistemnaya inzheneriya i informacionnye tekhnologii, 2023. T. 5, № 4 (13). –S. 50–76. DOI: 10.54708/2658-5014-SIIT-2023-no3-p50

5. Vasil'ev V.I., Kirillova A.D., Kuharev S.N. Kiberbezopasnost' avtomatizirovannyh sistem upravleniya promyshlennyh ob"ektov (sovremennoe sostoyanie, tendencii)//V.I. Vasil'ev, A.D. Kirillova, S.N. Kuharev / Vestnik UrFO. Bezopasnost' v informacionnoj sfere, 2018. T. 30. Vyp. 4. –S. 66–74. DOI: 10.14529/secur180410

6. Vasil'ev V.I., Kirillova A.D., Vul'fin A.M. Kognitivnoe modelirovanie vektora kiberatak na osnove metashablonov CAPEC//V.I. Vasil'ev, A.D. Kirillova, A.M. Vul'fin/ Voprosy kiberbezopasnosti, 2021. T. 42. Vyp. 2. S. 2–16. DOI: 10.21681/2311-3456-2021-2-2-16

7. Vasil'ev V.I., Vul'fin A.M., Guzairov M.B., Kirillova A.D. Interval'noe ocenivanie informacionnyh riskov s pomoshch'yu nechetkih seryh kognitivnyh kart//V.I. Vasil'ev, A.M. Vul'fin, M.B. Guzairov, A.D. Kirillova/ Informacionnye tekhnologii, 2018. T. 24. Vyp. 10. –S. 657–664. DOI: 10.17587/it.24.657-664

8. Anikin I.V. Metody i algoritmy kolichestvennoj ocenki i upravleniya riskami bezopasnosti v korporativnyh informacionnyh setyah na osnove nechetkoj logiki//I.V. Anikin/ Sistemnaya inzheneriya i informacionnye tekhnologii, 2023. T. 5, Vyp. 3. № 12. –S. 93–113. DOI 10.54708/2658-5014-SIIT-2023-no3-p93

9. Makarenko S.I. Kriterii i pokazateli ocenki kachestva testirovaniya na proniknovenie//S.I. Makarenko/ Voprosy kiberbezopasnosti, 2021. № 3(43). –S. 43–57. DOI:10.21681/2311-3456-2021-3-43-57

10. Smirnov S.I., Eremeev M.A., Magomedov SH.G., Izergin D.A. Kriterii i pokazateli ocenivaniya kachestva provedeniya rassledovaniya incidenta informacionnoj bezopasnosti pri celevoj kiberatake// S.I. Smirnov, M.A. Eremeev, SH.G. Magomedov, D.A. Izergin /Russian Technological Journal, 2024. T. 12. Vyp. 3. –S. 25–36. DOI: https://doi.org/10.32362/2500-316X-2024-12-3-25-36

11. Makarenko S. I., Smirnov G. E. Metodika obosnovaniya testovyh informacionno-tekhnicheskih vozdejstvij, obespechivayushchih racional'nuyu polnotu audita zashchishchennosti ob"ekta kriticheskoj informacionnoj infrastruktury//S. I. Makarenko, G. E. Smirnov/ Voprosy kiberbezopasnosti. 2021. № 6. (46). –S. 12–25. DOI:10.21681/2311-3456-2021-6-12-25

12. Kotenko I.V. i dr. Tekhnologii bol'shih dannyh dlya korrelyacii sobytij bezopasnosti na osnove ucheta tipov svyazej//I.V. Kotenko, A.V. Fedorchenko, I.B. Saenko, A.G. Kushnerevich A.G./ Voprosy kiberbezopasnosti,YU 2017. №5 (24). –S. 2–16. DOI: 10.21681/2311-3456-2017-5-2-16

13. Organizaciya sistemy setevogo monitoringa i ocenki sostoyaniya informacionnoj bezopasnosti ob"ekta / A.L. Maruhlenko, K.D. Seleznyov, M.O. Tanygin, L.O. Maruhlenko // Izvestiya YUgo-Zapadnogo gosudarstvennogo universiteta, 2019. T. 23. № 1. –S. 118–129. DOI: 10.21869/2223-1560-2019-23-1118-129.

14. Kobzar' A.I. Prikladnaya matematicheskaya statistika. Dlya inzhenerov i nauchnyh rabotnikov. –2-e izd., ispr. –M.: FIZMATLIT, 2012. –816 s.

15. URL: https://CVEform.mitre.org (Data obrashcheniya: 22.12.2025).

16. URL: https://attack.mitre.org/ (Data obrashcheniya: 22.12.2025).

17. URL: https://d3fend.mitre.org/ (Data obrashcheniya: 22.12.2025.

18. Bank dannyh ugroz bezopasnosti informacii// URL: https://bdu.fstec.ru/threat (Data obrashcheniya: 22.12.2025).

19. Metodicheskij dokument «Metodika ocenki ugroz bezopasnosti informacii» (utv. FSTEK 05.02.2021 g.)// URL: https://www.consultant.ru/document/cons_doc_LAW_378330/ (Data obrashcheniya: 22.12.2025).

20. Kocaman Yu., Gönen S., Barişkan M.A., Karacayilmaz G., Yilmaz E.N. A Novel approach to continuous CVE analysis on enterprise operating systems for vulnerability assessment. International journal of information technology (Singapore), 2022. Vol. 14. № 3. P. 1433–1443.

21. Aghaei E, Al-Shaer E, Shadid W, Niu X. Automated cve analysis for threat prioritization and impact prediction. 2023. arXiv preprint arXiv:2309.03040. DOI: https://doi.org/10.48550/arXiv.2309.03040

22. Manjunatha A, Kota K, Babu AS, et al. Cve severity prediction from vulnerability description-a deep learning approach. Procedia Comput Sci, 2024; 235:3105–17. DOI: 10.1016/j.procs.2024.04.294

23. Sonmeza F. O., C. Hankina, Malacariab P. Dynamics: An Automatic Attack Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases. Preprint submitted to Computers and Security September 26, 2022. 22 p. URL: https://www.researchgate.net/publication/364096733_Attack_Dynamics_An_Automatic_Attack_Graph_Generation_Framework_Based_on_System_Topology_CAPEC_CWE_and_CVE_Database

24. Tulinov I.S., Gubskov YU.A., Gromov YU.YU., SHatskih V.V. Formirovanie bazy dannyh uyazvimostej programmnogo obespecheniya dlya operativnoj nejtralizacii ugroz// I.S. Tulinov, YU.A. Gubskov, YU.YU. Gromov YU.YU., V.V. SHatskih/ Promyshlennye ASU i kontrollery, 2018, № 3. –S. 26–30.

25. Paiva R. Cernambi Virgem Ecológico (CVE), un nuevo caucho de extracción natural con calidad y directo de la selva amazónica a la industria del calzadohttps. DOI://doi.org/10.4067/S0718-07642021000600101

26. Belkin S.A., Belov V.M., Pivkin E.N. Primenenie faktornogo planirovaniya eksperimenta dlya ocenki veroyatnostej ugroz informacionnoj bezopasnosti// Polzunovskij vestnik, 2014. № 2. –S. 232–234.

27. Pletnev P. V., Belov V. M., Zubkov E. V., Kryzhanovskaya O. A. K voprosu ob opredelenii ugroz i riskov informacionnoj bezopasnosti s ispol'zovaniem scenarnogo podhoda i faktornogo planirovaniya eksperimenta// Vestnik SibGUTI. 2016. № 4. –C. 12–18.

28. Markelova E.B., Troeglazova A.V. Ocenka faktorov, okazyvayushchih vliyanie na realizaciyu ugroz informacionnoj bezopasnosti// INTEREKSPO GEO-SIBIR', 2023. T. 6. № 1. –S. 165–170.

29. SHago F.N. Metodika ocenki effektivnosti sistemy menedzhmenta informacionnoj bezopasnosti (SMIB) po vremeni reakcii sistemy na incidenty IB//Nauchno-tekhnicheskij vestnik informacionnyh tekhnologij, mekhaniki i optiki (Scientific and Technical Journal of Information Technologies, Mechanics and Optics), 2014. № 4 (92). –C. 115–123.

30. URL://www.anti-malware.ru/files/27-04-2023/28_s.jpg (Data obrashcheniya: 22.12.2025).

31. URL: https://d3fend.mitre.org/technique/d3f:HostReboot/ (Data obrashcheniya: 21.12.2025).

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, профессор Учебно-научного центра «Информационная безопасность» Федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

САФИУЛЛИН Николай Тахирович, кандидат технических наук, доцент Учебно-научного центра «Информационная безопасность» Федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: n.t.safiullin@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor, Professor of the Educational and Scientific Center «Information Security» of the Federal State Autonomous

Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: s.v.porshnev@urfu.ru

SAFIULLIN Nikolai Tahirovich, Candidate of Technical Sciences, Associate Professor of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: n.t.safiullin@urfu.ru