УДК 004.056
doi: 10.26583/bit.2024.3.04

Сергей В. Скрыль[1], Анастасия А. Ицкова[2], Кирилл Е. Ушаков[3]
Московский государственный технический университет им. Н.Э. Баумана,
2-я Бауманская, 5, Москва, 105005, Россия
[1]e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255
[2]e-mail: itskova@bmstu.ru, https://orcid.org/0009-0006-8436-5104
[3]e-mail: ushakovke@student.bmstu.ru, https://orcid.org/0009-0009-7811-938X

О ВОЗМОЖНОСТИ СОВЕРШЕНСТВОВАНИЯ ПРОЦЕДУР КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Аннотация. В статье формируется функциональная модель механизмов защиты от несанкционированного доступа (НСД) на объектах информационной инфраструктуры (КИИ). Определяется содержание мер защиты, применяемых при этом техник и этапов их реализации. Обосновывается порядок выполнения отдельных функциональных компонент структурного представления целевой функции «Защиты информации объектов КИИ от НСД». Иллюстрируется последовательность реализации этих компонент в виде смены состояний марковского процесса построения такой модели. Приводится таблица соответствия перечня процедур, выполняемых нарушителем в процессе реализации угрозы НСД к информации объекта КИИ процедурам защиты информации, демонстрируется возможность перехода от описания мер защиты информации от НСД на объектах КИИ в терминах функционального моделирования к математическому представлению временных характеристик функциональных компонент целевой функции защиты. Приводятся соответствующие аналитические выражения для различных вариантов представления порядка выполняемых функциональных компонент.

Ключевые слова: защита от несанкционированного доступа, объект критической информационной инфраструктуры, функциональное моделирование, функциональные компоненты, временные характеристики функциональных компонент.
Для цитирования: СКРЫЛЬ, Сергей В.; ИЦКОВА, Анастасия А.; УШАКОВ, Кирилл Е. О ВОЗМОЖНОСТИ СОВЕРШЕНСТВОВАНИЯ ПРОЦЕДУР КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Безопасность информационных технологий, [S.l.], т. 31, № 3, с. 94–104, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1680. DOI: http://dx.doi.org/10.26583/bit.2024.3.04.

Sergey V. Skryl[1], Anastasiya A. Itskova[2], Kirill E. Ushakov[3]
Bauman Moscow State Technical University,
2nd Baumanskaya str., 5, Moscow, 105005, Russia
[1]e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255
[2]e-mail: itskova@bmstu.ru, https://orcid.org/0009-0006-8436-5104
[3]e-mail: ushakovke@student.bmstu.ru, https://orcid.org/0009-0009-7811-938X

On the possibility of improving the procedures for quantifying information protection of critical information infrastructure objects from threats of unauthorized access

Abstract. The article develops a functional model of unauthorized access (UA) protection mechanisms at information infrastructure objects (IIOs). It defines the content of protection measures, techniques used, and stages of their implementation. It substantiates the order of execution of individual functional components of the structural representation of the objective function "Protection of information of IIOs

from UA". The sequence of implementation of these components is illustrated as a change in the states of the Markov process for constructing such a model. A table is provided of the correspondence between the list of procedures performed by an intruder in the process of implementing an UA threat to information of an IIOs and the procedures for protecting information, and it demonstrates the possibility of transition from the description of information protection measures from UA at IIOs in terms of functional modeling to the mathematical representation of the time characteristics of the functional components of the objective function of protection. The corresponding analytical expressions are provided for various options for representing the order of the functional components performed.
Keywords: unauthorized access, critical information infrastructure, functional modeling, functional components, temporal characteristics of functional components of the threat.
For citation: SKRYL, Sergey V.; ITSKOVA, Anastasiya A.; USHAKOV, Kirill E. On the possibility of improving the procedures for quantifying information protection of critical information infrastructure objects from threats of unauthorized access. IT Security (Russia), [S.l.], v. 31, no. 3, p. 94–104, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1680. DOI: http://dx.doi.org/10.26583/bit.2024.3.04.

Введение

В [1] приводятся результаты декомпозиции целевой функции угроз несанкционированного доступа (НСД) к информации объектов критической информационной инфраструктуры (КИИ). Это явилось предпосылкой для формализации действий нарушителя по реализации такого рода угроз с последующей количественной оценкой их временных характеристик.

Используя аналогичный подход, в данной статье исследуется возможность количественной оценки защищенности информации этих объектов от такого рода угроз.

1. Порядок построения функциональной модели мер защиты информации от НСД на объектах критической информационной инфраструктуры

Практика функционального моделирования механизмов обеспечения защиты информации от НСД [2–5] дает основание полагать, что процесс разработки функциональной модели реализуется в два этапа.

На первом этапе путем детализации целевой функции механизмов защиты от НСД на объектах КИИ образуются уровни ее функциональной декомпозиции. При этом будем исходить из того, что степень детализации, как и в предыдущем случае, будет определяться исходя из содержания методик ФСТЭК России, регламентирующих номенклатуру функциональных компонент защиты информации от НСД (табл. 1)[1].

[1]Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Таблица 1. Номенклатура функциональных компонент защиты информации от НСД

Используемые механизмы защиты информации	Классы защищенности				
	1Д	1Г	1В	1Б	1А
1	2	3	4	5	6
1. Средства управления доступом					
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:					
к ОИ	+	+	+	+	+
к терминалам, СВТ, узлам компьютерной сети, каналам связи, внешним устройствам СВТ	–	+	+	+	+
к программам	–	+	+	+	+
к данным	–	+	+	+	+
1.2. Управление потоками информации	–	–	+	+	+
2. Средства регистрации и учета					
2.1. Регистрация и учет:					
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	–	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	–	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по каналам связи	–	+	+	+	+
доступа программ субъектов доступа к терминалам, СВТ, узлам компьютерной сети,	–	+	+	+	+
каналам связи, внешним устройствам СВТ, программам и данным	–	+	+	+	+
изменения полномочий субъектов доступа	–	–	+	+	+
создаваемых защищаемых объектов доступа	–	–	+	+	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти СВТ и внешних накопителей	+	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	–	+	+	+	+
3. Криптографические средства					
3.1. Шифрование конфиденциальной информации	–	–	+	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	–	–	–	+	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	–	–	–	–	+
4. Средства обеспечения целостности рабочей среды СВТ					
4.1. Обеспечение целостности программных средств и обрабатываемой информации	–	–	–	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в информационной системе	+	+	+	+	+
4.4. Периодическое тестирование рабочей среды СВТ	–	–	+	+	+
4.5. Наличие средств восстановления информации	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	–	–	+	+	+

На втором этапе, как и в случае функциональной модели угрозы НСД, путем эмпирического исследования взаимосвязи между функциональными компонентами целевой функции защиты информации от такого рода угроз, на каждом из уровней декомпозиции целевой функции устанавливается порядок их реализации (выполнения).

При реализации первого этапа построения функциональной модели процессов функционирования механизмов защиты информации от НСД на объектах КИИ будем исходить из заявленного двухуровневого представления множества функций[1], реализуемых этими механизмами. Естественно полагать, что классификационными основаниями [6] в этом случае будут: меры защиты (*S*), применяемые при этом техники (*U*) и этапы их реализации (*W*).

При построении функциональной модели механизмов защиты информации от НСД на объектах КИИ воспользуемся существующими методиками ФСТЭК России относительно возможностей по обеспечению функций защиты[1] и сформируем множество функциональных компонент целевой функции защиты информации от НСД на объектах КИИ (рис. 1).

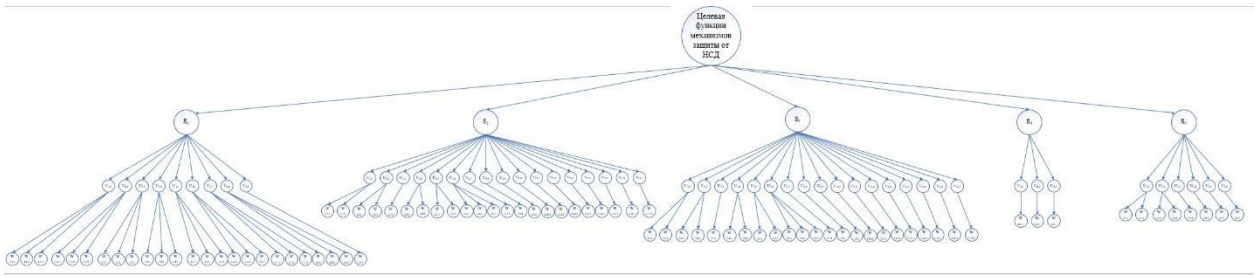

Рис. 1. Детализация целевой функции механизмов защиты от НСД на объектах КИИ

В соответствии со вторым этапом устанавливается порядок реализации функциональных компонент на каждом из представленных уровней (рис. 2–4).

Представленные в табл. 1 группы средств защиты информации будем в дальнейшем рассматривать как подсистемы защиты. Реализацию этими подсистемами своих функций представим как стратегии (S_i, i = 1, 2, …, 5) защиты информации от НСД.

На рис. 2 представлен порядок реализации целевой функции *D* – «Защита информации объектов КИИ от НСД» соответствующими функциональными компонентами (стратегиями):

S_1 – «Управление доступом»;
S_2 – «Регистрация действий субъектов доступа»;
S_3 – «Учет действий субъектов доступа»;
S_4 – «Криптографические преобразования»;
S_5 – «Обеспечение целостности операционной среды СВТ».

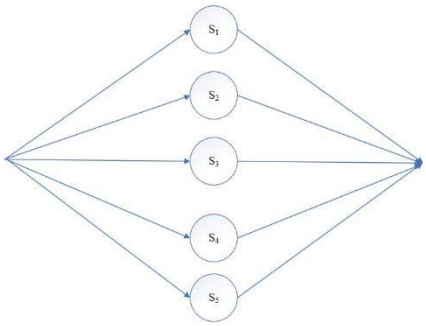

Рис. 2. Функциональное представление целевой функции «Механизм защиты от НСД на объектах КИИ»

Перечисленные стратегии реализуют определенные тактики защиты информации от НСД. Представление стратегий тактиками будем считать как второй уровень декомпозиционного представления целевой функции «Механизм защиты от НСД на объектах КИИ».

В качестве примера рассмотрим приводимый на рис. 3 порядок реализации функциональной компоненты S_1 – «Управление доступом» соответствующими ей функциональными компонентами следующего декомпозиционного уровня (техникам):

$U_{1.1}$ – «Управление доступом субъектов к объекту КИИ»;
$U_{1.2}$ – «Управление доступом субъектов к терминалам объекта КИИ»;
$U_{1.3}$ – «Управление доступом субъектов к СВТ объекта КИИ»;
$U_{1.4}$ – «Управление доступом субъектов к узлам компьютерной сети объекта КИИ»;
$U_{1.5}$ – «Управление доступом субъектов к каналам связи объекта КИИ»;
$U_{1.6}$ – «Управление доступом субъектов к внешним устройствам СВТ объекта КИИ»;
$U_{1.7}$ – «Управление доступом субъектов к программам объекта КИИ»;
$U_{1.8}$ – «Управление доступом субъектов к данным объекта КИИ»;
$U_{1.9}$ – «Управление потоками информации объекта КИИ».

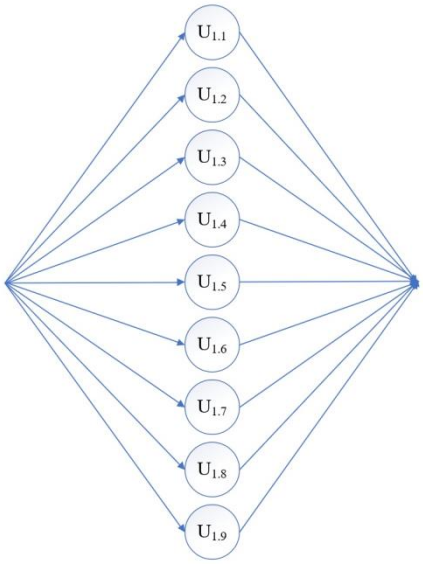

Рис. 3 Функциональное представление функциональной компоненты S_1 «Управление доступом»

Перечисленные тактики реализации мер защиты информации от НСД выполняются соответствующими этапами. В качестве примера рассмотрим приводимый на рис. 4 порядок реализации техники $U_{1.1}$ – «Управление доступом субъектов к объекту КИИ» ее функциональными компонентами (этапами):

$W_{1.1.1}$ – «Идентификация доступа субъектов к объекту КИИ»;
$W_{1.1.2}$ – «Проверка подлинности субъектов доступа к объекту КИИ»;
$W_{1.1.3}$ – «Контроль доступа субъектов к объекту КИИ».

Детализация целевой функции D – «Механизм защиты от НСД на объектах КИИ» позволяет сопоставить функциональные компоненты нижнего уровня ее детализации с функциональными компонентами нижнего уровня детализации целевой функции $Ц$ – «Угроза НСД к информации объекта КИИ». Это дает возможность идентифицировать те функции механизма защиты информации от НСД, которые обеспечивают оптимальный вариант реагирования на такого рода угрозу. В табл. 2 приведен перечень процедур, выполняемых нарушителем в процессе реализации угрозы НСД к информации объекта

КИИ [1], соответствующих тем этапам реализации механизмов защиты информации, которые рассмотрены в данной статье в качестве примеров.

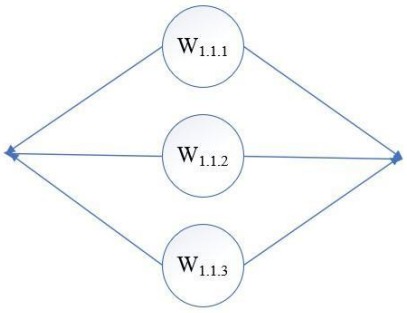

Рис. 4. Порядок реализации техники $U_{1.1}$ – «Управление доступом субъектов к объекту КИИ»

2. Построение математических выражений, для оценки средних значений времени реализации функциональных компонент защиты информации от НСД на объектах КИИ

Полученные результаты декомпозиции функционального описания целевой функции мер защиты информации от НСД на объектах КИИ следует рассматривать как формализованное представление данной целевой функции для построения математических выражений, позволяющих оценивать средние значения времени реализации ее функциональных компонент.

Для этого воспользуемся функциональными соответствиями между:

временем выполнения этапов и временем выполнения техник, реализующих эти этапы;

временем выполнения техник и временем реализации мер защиты, реализующих эти техники;

временем реализации мер защиты и временем реализации целевой функции в целом.

Указанные соответствия, а, следовательно, и вид математических выражений для указанных временных характеристик определяются содержанием композиционных связей между реализуемыми функциональными компонентами.

При построении математических выражений для определения средних значений времени реализации функциональных компонент целевой функции мер защиты информации от НСД к объектам КИИ, как и в случае [1] воспользуемся свойством линейности и аддитивности, математического ожидания композиции случайных величин [7-10]. При этом для композиции случайных величин $/(\Phi_1)$, $/(\Phi_2)$, …, $/(\Phi_N)$, характеризующих время реализации последовательности функциональных компонент Φ_1, Φ_2, …, Φ_N, воспользуемся выражением:

$$\underline{\omega}\,(\Phi^{(+1)}) = \sum_{n=1}^{N} \underline{\tau}\,(\Phi_n), \qquad (1)$$

где $\underline{\tau}\,(\Phi_n)$ – среднее значение случайной величины $/(\Phi_n)$ времени реализации n-ой функциональной компоненты;

$\Phi^{(+1)}$ – идентификатор функциональной компоненты, композиционно образованной на множестве функциональных компонент $\{\Phi_n\}$, $n = 1, 2, \ldots, N$;

$\underline{\tau}\,(\Phi^{(+1)})$ – среднее время реализации функциональной компоненты $\Phi^{(+1)}$.

Таблица 2. Процедуры, выполняемые нарушителем в процессе реализации угрозы НСД к информации объекта КИИ

№ №	Наименование процедуры, выполняемой нарушителем в процессе реализации угрозы НСД к информации объекта КИИ	Идентификация процедуры угрозы	Наименование этапа реализации механизма защиты информации, соответствующей реагированию на процедуру угрозы	Идентификация этапа реализации механизма защиты информации
1.	Загрузка альтернативной ОС с нештатного носителя	$П_{1.1.3.1}$	Идентификация доступа субъектов к объекту КИИ	$W_{1.1.1}$
2.	Запуск программного продукта, отключающего пароль, записанного на CD-диск с функцией автозапуска	$П_{1.3.3.1}$	Идентификация доступа субъектов к объекту КИИ	$W_{1.1.1}$
3.	Создание новой учетной записи с расширенными привилегиями посредством документированных возможностей ОС	$П_{1.4.3.1}$	Идентификация доступа субъектов к объекту КИИ	$W_{1.1.1}$
4.	Запуск программного продукта, выявляющего пароль, записанного на внешний носитель	$П_{1.3.2.1}$	Проверка подлинности субъектов доступа к объекту КИИ	$W_{1.1.2}$
5.	Выявление пароля BIOS при загруженной ОС, посредством использования программ выявления пароля	$П_{1.4.1.1}$	Проверка подлинности субъектов доступа к объекту КИИ	$W_{1.1.2}$
6.	Уничтожение системного реестра	$П_{1.4.4.1}$	Проверка подлинности субъектов доступа к объекту КИИ	$W_{1.1.2}$
7.	Подбор пароля BIOS путем перебора вручную на основе собранных данных о пользователе	$П_{1.1.1.1}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
8.	Обход заданного пароля BIOS путем обесточивания материнской платы	$П_{1.1.2.1}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
9.	Обход заданного пароля BIOS путем переключения джамперов с целью обнуления BIOS	$П_{1.1.2.2}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
10.	Обход заданного пароля BIOS путем подмены микросхемы BIOS	$П_{1.1.2.3}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
11.	Загрузка альтернативной ОС с нештатного носителя	$П_{1.1.3.1}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
12.	Подбор пароля доступа посредством ввода учетного имени и пароля, заданных по умолчанию, для используемой ОС	$П_{1.2.1.1}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
13.	Подбор пароля и учетного имени посредством перебора различных вариантов	$П_{1.2.1.2}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
14.	Перезапуск компьютера и попытка реализации тактик Т1.1 и Т1.2	$П_{1.3.4.1}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$
15.	Получение необходимой (защищаемой) информации пользователя	$П_{2.2.5.1}$	Контроль доступа субъектов к объекту КИИ	$W_{1.1.3}$

В случае, когда функциональные компоненты $Ф_1$, $Ф_2$, …, $Ф_K$, связаны параллельно, для композиции случайных величин $/(Ф_1)$, $/(Ф_2)$, …, $/(Ф_K)$, характеризующих время их реализации, будем использовать выражение:

$$\underline{\omega}(\Phi^{(+1)}) = \sum_{k=1}^{K} p(\Phi_k) \cdot \underline{\tau}(\Phi_k), \quad (2)$$

где $p(\Phi_k)$ – вероятность выполнения функциональной компоненты Φ_k.

На основе обобщенного представления временных характеристик в виде выражений (1) и (2) сформируем выражения для определения временных характеристик функциональных компонент, составляющих декомпозиционную структуру целевой функции мер защиты информации от НСД на объектах КИИ [11-14].

В качестве примера будем использовать проиллюстрированные выше функциональные компоненты.

Выражение (3), полученное в соответствии с приведенным на рис. 4 функциональным представлением техники $U_{1.1}$ – «Управление доступом субъектов к объекту КИИ», является выражением для определения среднего значения случайной величины времени $\underline{\omega}(U_{1.1})$, затрачиваемого на реализацию данной техники:

$$\underline{\omega}(U_{1.1}) = p(W_{1.1.1}) \cdot \underline{\tau}(W_{1.1.1}) + p(W_{1.1.2}) \cdot \underline{\tau}(W_{1.1.2}) + + p(W_{1.1.3}) \cdot \underline{\tau}(W_{1.1.3}), \quad (3)$$

где $p(W_{1.1.1})$ и $\underline{\tau}(W_{1.1.1})$ – вероятность выполнения и среднее значение времени реализации этапа $W_{1.1.1}$ – «Идентификация доступа субъектов к объекту КИИ»;

$p(W_{1.1.2})$ и $\underline{\tau}(W_{1.1.2})$ – вероятность выполнения и среднее значение времени реализации этапа $W_{1.1.2}$ – «Проверка подлинности субъектов доступа к объекту КИИ;

$p(W_{1.1.3})$ и $\underline{\tau}(W_{1.1.3})$ – вероятность выполнения и среднее значение времени реализации этапа $W_{1.1.3}$ – «Контроль доступа субъектов к объекту КИИ».

Выражение (4), полученное в соответствии с приведенным на рис. 3 функциональным представлением меры S_1 – «Управление доступом», является выражением для определения среднего значения случайной величины времени $\underline{\omega}(S_1)$, затрачиваемого нарушителем на реализацию данной тактики [15-18]:

$$\underline{\omega}(S_1) = p(U_{1.1}) \cdot \underline{\tau}(U_{1.1}) + p(U_{1.2}) \cdot \underline{\tau}(U_{1.2}) + p(U_{1.3}) \cdot \underline{\tau}(U_{1.3}) + \\ + p(U_{1.4}) \cdot \underline{\tau}(U_{1.4}) + p(U_{1.5}) \cdot \underline{\tau}(U_{1.5}) + p(U_{1.6}) \cdot \underline{\tau}(U_{1.6}) + p(U_{1.7}) \cdot \underline{\tau}(U_{1.7}) + + p(U_{1.8}) \cdot \\ \underline{\tau}(U_{1.8}) + p(U_{1.9}) \cdot \underline{\tau}(U_{1.9}), \quad (4)$$

где $p(U_{1.1})$ и $\underline{\tau}(U_{1.1})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.1}$ – «Управление доступом субъектов к объекту КИИ;

$(U_{1.2})$ и $\underline{\tau}(U_{1.2})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.2}$ – «Управление доступом субъектов к терминалам объекта КИИ»;

$(U_{1.3})$ и $\underline{\tau}(U_{1.3})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.3}$ – «Управление доступом субъектов к СВТ объекта КИИ»;

$(U_{1.4})$ и $\underline{\tau}(U_{1.4})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.4}$ – «Управление доступом субъектов к узлам компьютерной сети объекта КИИ»;

$(U_{1.5})$ и $\underline{\tau}(U_{1.5})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.5}$ – «Управление доступом субъектов к каналам связи объекта КИИ»;

$(U_{1.6})$ и $\underline{\tau}(U_{1.6})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.6}$ – «Управление доступом субъектов к внешним устройствам СВТ объекта КИИ»;

$(U_{1.7})$ и $\underline{\tau}(U_{1.7})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.7}$ – «Управление доступом субъектов к программам объекта КИИ»;

$(U_{1.8})$ и $\underline{\tau}(U_{1.8})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.8}$ – «Управление доступом субъектов к данным объекта КИИ»;

$(U_{1.9})$ и $\underline{\tau}(U_{1.9})$ – вероятность выполнения и среднее значение времени реализации техники $U_{1.9}$– «Управление потоками информации объекта КИИ».

Выражение (5), полученное в соответствии с приведенным на рис. 2 функциональным представлением целевой функции *D* – «Защита информации объектов КИИ от НСД», является выражением для определения среднего значения случайной величины времени $\underline{\omega}(D)$, затрачиваемого на реализацию данной целевой функции:

$$\underline{\omega}(D)=p(S_1)\cdot\underline{\tau}(S_1)+p(S_2)\cdot\underline{\tau}(S_2)+p(S_3)\cdot\underline{\tau}(S_3)+p(S_4)\cdot\underline{\tau}(S_4)+p(S_5)\cdot\underline{\tau}(S_5),.(5)$$

где $p(S_1)$ и $\underline{\tau}(S_1)$ – вероятность выполнения и среднее значение времени реализации мер защиты S_1– «Управление доступом»;

$p(S_2)$ и $\underline{\tau}(S_2)$ – вероятность выполнения и среднее значение времени реализации мер защиты S_2 – «Регистрация действий субъектов доступа»;

$p(S_3)$ и $\underline{\tau}(S_3)$ – вероятность выполнения и среднее значение времени реализации мер защиты S_3 – «Учет действий субъектов доступа»;

$p(S_4)$ и $\underline{\tau}(S_4)$ – вероятность выполнения и среднее значение времени реализации мер защиты S_4 – «Криптографические преобразования»;

$p(S_5)$ и $\underline{\tau}(S_5)$ – вероятность выполнения и среднее значение времени реализации мер защиты S_5 – «Обеспечение целостности операционной среды СВТ».

Заключение

На основании практики использования функционального моделирования, как инструмента первичной формализации исследуемых процессов, полученные результаты позволяют описать угрозы НСД к информации объектов КИИ и работу механизмов защиты от такого рода угроз терминами марковских процессов, сформировать комплекс математических моделей по оценке временных характеристик угроз НСД к информации и механизмов ее защиты от такого рода угроз, разработать математические модели показателей защищенности информации от НСД этих объектов.

СПИСОК ЛИТЕРАТУРЫ:

1. Скрыль, Сергей В.; Ицкова, Анастасия А.; Хасин, Евгений В. О возможности совершенствования процедур количественной оценки угроз несанкционированного доступа к информации объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 30, № 4, с. 61–73, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.4.03.
2. Скрыль С.В., Сычев В.М., Мещерякова Т.В., Гайфулин В.В., Суворов А.А. Методические аспекты построения функциональной модели угроз несанкционированного доступа к компьютерной информации. Промышленные АСУ и контроллеры. 2019, № 11, с. 48–59. DOI: 10.25791/asu.11.2019.998. – EDN: EJKVAK.
3. Скрыль С.В., Карпычев В.Ю., Потанин В.Е. Формальные основы функционального моделирования вредоносных воздействий на защищенные информационные системы в интересах выявления противоправных действий в сфере компьютерной информации. Наука производству. № 3(89), 2006, с. 30–31. – EDN: HTJASV.
4. Скрыль С.В. и др. Функциональное моделирование как методология исследования конфиденциальности информационной деятельности. Интеллектуальные системы (INTELS’ 2010): Труды Девятого международного симпозиума. М.: МГТУ им. Н.Э. Баумана. 2010, С. 590–593.

5. Волкова С.Н., Дерябин А.С. Функциональное моделирование, как инструмент исследования механизмов защиты информации. Информация и безопасность. Воронеж: ВГТУ. 2010, Вып. 2, с. 303–304. – EDN: MSYGIB.
6. Сычев А.М. и др. Классификационные основания для синтеза системы характеристик эффективности мер реагирования на угрозы безопасности электронного банкинга. Промышленные АСУ и контроллеры. 2017, № 7, с. 44–52. – EDN: ZCQGJV.
7. Корн Г., Корн Т. Справочник по математике (для научных работников и инженеров). М: Наука, 1974. – 832 с.
8. Тихонов В.И., Миронов М.А. Марковские процессы. М.: Сов. радио, 1977. – 488 с.
9. Чжун Кай-лай. Однородные цепи Маркова. Перев. с англ. – М.: Мир, 1964. – 425 с.
10. Кемени Дж. Дж., Снелл Дж. Л. Конечные цепи Маркова. Перев. с англ. М.: Наука. 1970. – 272 с.
11. Сычев А.М., Гайфулин В.В., Зеленцов В.В., Пономарев М.В., Тегенцев И.М. Основные теоретические положения методологии оценки характеристик мер обеспечения безопасности информации. Авиакосмическое приборостроение. 2018, № 8, с. 46–53. – EDN: ALESTB.
12. Скрыль С.В. и др. Математические модели временных характеристик угроз несанкционированного доступа к компьютерной информации. Промышленные АСУ и контроллеры. 2019, № 11, с. 60–65. DOI: 10.25791/asu.11.2019.999. – EDN: PEUEDV.
13. Сычев А.М. и др. Оценка защищенности информации от вирусных атак: Существующий и перспективный методический аппарат. Промышленные АСУ и контроллеры. 2018, № 9, с. 51–62. – EDN: YABXKX.
14. Пономаренко С.А., Скрыль С.В. Математическое моделирование как инструмент исследования механизмов защиты информации. Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: материалы Всероссийской научно-практической конференции. Ч. 2. Воронеж: Воронежский институт МВД России. 2014, с. 169–171. – EDN: UQBVRT.
15. Джоган, В.К.; Курило, А.П. Защищенность информационных ресурсов компьютерных систем как система показателей эффективности защиты информации. Безопасность информационных технологий, [S.l.], т. 18, №. 4, с. 164–169, 2011. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/606 (дата обращения: 27.05.2024).
16. Джоган, В.К.; Курило, А.П.; Шимон, Н.С. Особенности синтеза системы показателей эффективности защиты информации в компьютерных системах. Безопасность информационных технологий, [S.l.], т. 18, № 4, с. 170–175, 2011. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/607 (дата обращения: 27.05.2024).
17. Сычев А.М. и др. Проблема синтеза системы показателей для оценки качества защиты информации / Вопросы защиты информации. М.: Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт межотраслевой информации – Федеральный информационно-аналитический центр оборонной промышленности». 2010, № 4, с. 51–57. – EDN: MWFALJ.
18. Никулин С.С., Сычев А.М. Требования к методологическому аппарату синтеза системы характеристик качества обеспечения защиты информации. Вестник Воронежского института МВД России. Воронеж: Воронежский институт МВД России. 2015, №. 1, с. 96–104. URL: https://cyberleninka.ru/article/n/trebovaniya-k-metodologicheskomu-apparatu-sinteza-sistemy-harakteristik-kachestva-obespecheniya-zaschity-informatsii (дата обращения: 27.05.2024).

REFERENCES:

[1] Skryl, Sergey V.; Itskova, Anastasiya A.; Khasin, Evgeny V. The possibility of improving procedures for quantitative threat assessment of unauthorized access to information of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 30, no. 4, p. 61–73, 2023. DOI: http://dx.doi.org/10.26583/bit.2023.4.03 (in Russian).
[2] Skryl S.V., Sychev V.M., Meshcheryakova T.V., Gaifulin V.V., Suvorov A.A. Methodological aspects of constructing a functional model of threats of unauthorized access to computer information. Industrial ACS and Controllers. 2019, no. 11, p. 48–59. DOI: 10.25791/asu.11.2019.998 (in Russian). – EDN: EJKVAK.
[3] Skryl S.V., Karpychev V.Yu., Potanin V.E. Formal Foundations of Functional Modeling of Malicious Impacts on Protected Information Systems to Identify Unlawful Actions in the Field of Computer Information // Science for Production. No. 3(89), 2006, p. 30–31 (in Russian). – EDN: HTJASV.
[4] Skryl S.V. et al. Functional Modeling as a Methodology for Studying the Confidentiality of Information Activities. Intelligent Systems (INTELS' 2010): Proceedings of the Ninth International Symposium. M.: Bauman Moscow State Technical University. 2010, p. 590–593 (in Russian).

[5] Volkova S.N., Deryabin A.S. Functional modeling as a tool for studying the mechanisms of information protection. Information and security. Voronezh: VSTU. 2010, Issue. 2, p. 303–304 (in Russian). – EDN: MSYGIB.
[6] Sychev A.M. et al. Classification Grounds for Synthesizing the System of Characteristics for the Effectiveness of Measures Responding to Security Threats in Electronic Banking. Industrial ACS and Controllers. 2017, no. 7, p. 44–52 (in Russian). – EDN: ZCQGJV.
[7] Korn G., Korn T. Handbook of Mathematics (for Scientists and Engineers). M.: Nauka, 1974. – 832 p. (in Russian).
[8] Tikhonov V.I., Mironov M.A. Markov Processes. M.: Soviet Radio, 1977. – 488 p. (in Russian).
[9] Chung Kai-lai. Homogeneous Markov Chains. Translated from English. M.: Mir, 1964. – 425 p. (in Russian).
[10] Kemeny J.G., Snell J.L. Finite Markov Chains. Translated from English. M.: Nauka, 1970. – 272 p. (in Russian).
[11] Sychev A.M., Gaifulin V.V., Zelentsov V.V., Ponomarev M.V., Tegentsev I.M. Basic Theoretical Provisions of the Methodology for Assessing the Characteristics of Information Security Measures. Aerospace Instrumentation. 2018, no. 8, p. 46–53 (in Russian). – EDN: ALESTB.
[12] Skryl S.V. et al. Mathematical models of the temporal characteristics of threats of unauthorized access to computer information. Industrial ACS and Controllers. 2019, no. 11, p. 60–65. DOI: 10.25791/asu.11.2019.999 (in Russian). – EDN: PEUEDV.
[13] Sychev A.M. et al. Evaluation of information security from virus attacks: existing and future methodological apparatus. Industrial ACS and Controllers. 2018, no. 9, p. 51–62 (in Russian). – EDN: YABXKX.
[14] Ponomarenko S.A., Skryl S.V. Mathematical Modeling as a Tool for Studying Information Protection Mechanisms. Current Issues of Security Systems Operation and Protected Telecommunication Systems: Materials of the All-Russian Scientific and Practical Conference. Part 2. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russi. 2014, p. 169–171 (in Russian). – EDN: UQBVRT.
[15] Dzhogan, V.K.; Kurylo, A.P. Protection of Information Resources of Computer Systems as a System of Performance Data Protection. IT Security (Russia), [S.l.], v. 18, no. 4, p. 164–169, 2011. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/606 (accessed: 27.05.2024) (in Russian).
[16] Dzhogan, V.K.; Kurylo, A.P.; Shimon, N.S. Features of the Synthesis of Performance Security Information in Computer Systems. IT Security (Russia), [S.l.], v. 18, no. 4, p. 170–175, 2011. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/607 (accessed: 27.05.2024) (in Russian).
[17] Sychev A.M. et al. Problem of synthesis of the system of metrics for the estimation qualities of protection of the information. Information Security Issues. Moscow: Federal State Unitary Enterprise "All-Russian Research Institute of Intersectoral Information – Federal Information and Analytical Center of the Defense Industry". 2010, no. 4, p. 51–57 (in Russian). – EDN: MWFALJ.
[18] Nikulin S.S., Sychev A.M. Requirements for the Methodological Apparatus for Synthesizing the System of Information Security Quality Assurance Characteristics. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2015, no. 1, p. 96–104. URL: https://cyberleninka.ru/article/n/trebovaniya-k-metodologicheskomu-apparatu-sinteza-sistemy-harakteristik-kachestva-obespecheniya-zaschity-informatsii (accessed: 27.05.2024) (in Russian).

Поступила в редакцию – 27 мая 2024 г. Окончательный вариант – 26 июля 2024 г.
Received – May 27, 2024. The final version – Jule 26, 2024.