УДК 004.056

Сергей В. Скрыль[1], Анастасия А. Ицкова[2], Евгений В. Хасин[3]
[1,2]Московский государственный технический университет им. Н.Э. Баумана,
2-я Бауманская, 5, Москва, 105005, Россия
[3]Минцифры России,
Пресненская наб., 10, стр. 2, Москва, 123112, 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: e.khasin@digital.gov.ru, https://orcid.org/0009-0007-1581-3660

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

DOI: http://dx.doi.org/10.26583/bit.2023.4.03

Аннотация. Определяется содержание основных этапов оценки угроз несанкционированного доступа (НСД) на объектах критической информационной инфраструктуры (КИИ), на основании анализа основных положений Методики оценки угроз безопасности информации ФСТЭК России. Акцентируется внимание на путях развития методологии оценки угроз безопасности информации. Предлагается функционально ориентированный подход для учета динамики реализации угроз НСД к информации объектов КИИ. Рассматривается алгоритм построения функциональной модели угрозы, основанный на существующей ее структуризации в рамках представленной в документах ФСТЭК России базовой модели угроз безопасности информации. Обосновывается декомпозиционная иерархическая структура целевой функции угрозы, как первый этап построения модели. Приводится содержание уровней структуры: целевой функции угрозы, стратегий ее реализации, используемых тактик, этапов действий нарушителя и выполняемых процедур доступа к операционной среде компьютерной системы и деструктивного воздействия на информацию. Определяется последовательность выполнения отдельных функциональных компонент структуры и иллюстрируется порядок реализации, в виде смены состояний марковского процесса, как второй этап построения такой модели. На основе предложенного представления демонстрируется возможность перехода от описания угрозы НСД к информации объекта КИИ в терминах функционального моделирования к математическому представлению временных характеристик функциональных компонент ее целевой функции. Приводятся полученные аналитические выражения для различных вариантов представления порядка выполняемых функциональных компонент.

Ключевые слова: несанкционированный доступ, критическая информационная инфраструктура, функциональное моделирование, функциональные компоненты, временные характеристики функциональных компонент угрозы.

Для цитирования: 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. URL: https://bit.spels.ru/index.php/bit/article/view/1549. DOI: http://dx.doi.org/10.26583/bit.2023.4.03.

Sergey V. *Skryl*[1], Anastasiya A. Itskova[2], Evgeny V. Khasin[3]
[1,2]Bauman Moscow State Technical University,
2nd Baumanskaya str., 5, Moscow, 105005, Russia
[3]Ministry of Digital Development of Russia,
Presnenskaya embankment, 10, building 2, Moscow, 123112, 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: e.khasin@digital.gov.ru, https://orcid.org/0009-0007-1581-3660

The possibility of improving procedures for quantitative threat assessment of unauthorized access to information of critical information infrastructure facilities

DOI: http://dx.doi.org/10.26583/bit.2023.4.03

Abstract. The content of the main threat assessment stages of unauthorized access (UA) at critical information infrastructure (CII) facilities is determined on the basis of analysis of the primary provisions of the Methodology for Assessing Information Security Threats, approved on February 5, 2021 by the FSTEC of Russia. The ways to develop a methodology for assessing such information security threats are focused. A functionally-oriented approach is proposed to take into account the dynamics of the UA threat implementation regarding information of CII facilities. The procedure for constructing a functional model of the threat is considered in accordance with its existing structuring within the framework of the basic model of information security threats presented in the documents of the FSTEC of Russia. The decompositional hierarchical structure of the target threat function is substantiated as the first stage in constructing the model. The content of structure levels is given: the level of target threat function, the level of its implementation strategies, the level of tactics used, the level of the intruder's action stages, and the level of procedures done to access the operating environment of the computer system (CS) and destructive impact on information. The execution sequence of individual functional components of this structure is determined as well as the order of their implementation is illustrated in the form of a change of states of the Markov process as the second stage of constructing the model. Based on this vision, the possibility of moving from a description of the UA threat to information of CII facilities in terms of functional modeling to a mathematical representation of the temporal characteristics of functional components of its target function is demonstrated. The corresponding analytical expressions are given for various options for representing the order of executed functional components.

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.; 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. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1549. DOI: http://dx.doi.org/10.26583/bit.2023.4.03.

Введение

Существенный рост профессионализма иностранных спецслужб в сфере информационных технологий представляет серьезную угрозу для одного из наиболее социально значимых их приложений – критически важных объектов[1]. Формируемая в этих условиях критическая информационная инфраструктура (КИИ)[1] является значимым фактором в деятельности важнейших институтов государства. Естественно полагать, что материальный и репутационный ущерб от нарушения безопасности в среде КИИ является колоссальным. Этому способствуют объективно существующие уязвимости процедур хранения и обработки информации объектов КИИ к различного рода угрозам безопасности информации [1, 2]. Специфичность информационной среды объектов КИИ, как операционной среды компьютерных систем, в качестве угроз их безопасности определяет угрозы несанкционированного доступа (НСД) [3].

В соответствии с определением, под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации[2].

[1]Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Банк России, 2017. URL: https://base.garant.ru/71730198/ (дата обращения: 19.06.2023).

[2]ГОСТ Р 53114-2008. URL: https://protect.gost.ru/document.aspx?control=7&id=174974 (дата обращения: 19.06.23).

Естественно полагать, что эффективное предотвращение угроз НСД на объектах КИИ может осуществляться лишь в условиях всестороннего и системного исследования их источников, уязвимостей к проявлениям такого рода угроз и деструктивного воздействия на информацию [4].

1. «Методика оценки угроз безопасности информации» как концептуальная основа для системного исследования угроз несанкционированного доступа к информации объектов КИИ

В качестве концептуальной основы для такого исследования воспользуемся методическим документом «Методика оценки угроз безопасности информации», утвержденным 5 февраля 2021 г. ФСТЭК России[3]. Данная методика реализует сложившуюся на сегодняшний день концепцию определения угроз НСД, возникновение которых возможно на объектах КИИ.

Трактовка п. 2.15. методики применительно к оценке угроз НСД на объектах КИИ дает возможность определить ее следующие этапы:

1) определение негативных последствий для информационной деятельности объекта, которые могут наступить от реализации (возникновения) угроз НСД;

2) определение возможных объектов воздействия угроз НСД;

3) оценку возможности реализации (возникновения) угроз НСД и определение их актуальности.

Очевидно, что проблема всестороннего и системного исследования угроз НСД на объектах КИИ должна решаться в рамках третьего этапа. При этом, в соответствии с п. 1.6 методики, допускается разработка корпоративных методик оценки такого рода угроз, учитывающих особенности функционирования объектов КИИ в соответствующей области деятельности.

Следует заметить, что всестороннее и системное исследование угроз НСД на объектах КИИ преследует цель адекватного отражения их свойств в рамках определенной метрики [5]. Случайный характер условий возникновения угроз НСД, базирующийся на причинно-следственных отношениях между их источниками, уязвимостями компьютерной информации к возникновению такого рода угроз и их деструктивным воздействиям на операционную среду объектов КИИ, приводит к необходимости рассматривать в качестве такой метрики вероятность проявления угрозы.

Одним из направлений решения данной проблемы является количественная оценка угроз НСД в рамках рассмотрения их как актуальных. С этой целью воспользуемся положениями предыдущей версией «Методики оценки угроз безопасности информации» – «Методикой определения актуальных угроз безопасности информации».

В соответствии с положениями данной методики отнесение тех или иных субъектов к источникам угроз, осуществляется путем установления соответствия между целями деятельности этих субъектов и их возможностями. При этом процедура установления соответствия носит эмпирический характер [6–8].

К сожалению, несмотря на довольно глубокую проработку всех обстоятельств, связанных с возникновением угроз НСД и их вредоносным воздействием на информационные ресурсы и процессы в компьютерных системах, представленный методический аппарат не обеспечивает учет тех случайных состояний, которые характеризуют динамику такого рода угроз. На это непосредственно указывается в п. 5

[3]Методический документ ФСТЭК России «Методика оценки угроз безопасности информации». Утверждена 5 февраля 2021 г. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 19.06.2023).

методики «Определение вероятностей реализации угроз»: «вероятность угрозы характеризует динамику ее возникновения и реализации. … Такие модели в настоящее время отсутствуют, а их разработка представляет собой достаточно длительный процесс.

Для парирования сложностей, связанных с отсутствием математических моделей расчета вероятностей реализации угроз, принято следующее допущение: … вероятность реализации угрозы в условиях отсутствия мер защиты приравнивается к единице, если данная угроза имеет место, и к нулю, если угроза отсутствует. Последнее допущение равносильно тому, что выбирается такое время, за которое реально существующая угроза может быть реализована с вероятностью, близкой к единице. В последующем предполагается расширить данную методику путем разработки необходимых математических моделей расчета вероятности реализации угрозы и устранить данное допущение».

Анализируя «Методику оценки угроз безопасности информации», как концепцию исследования вопросов обеспечения безопасности объектов КИИ, можно выявить два весьма серьезных обстоятельства, требующих уточнения ряда ее положений при использовании в качестве концептуальной основы для количественной характеристики нарушения информационной безопасности этих объектов вследствие реализации угроз НСД.

Первое обстоятельство связано с эмпирическим характером процедуры оценки возможностей нарушителя по реализации угроз НСД к информации, основанной на экспертном анализе объектно-субъектных отношений между источниками такого рода угроз безопасности информации, ее уязвимостями к их реализации и нарушение состояний защищенности информации объектов КИИ. Описательный характер процедуры анализа и ее субъективизм как следствие влияния мнения экспертов на оценочные решения, не позволяет достоверно оценить, а, следовательно, и адекватно характеризовать, уровень угрозы. В этой связи представляется целесообразным проработка всех аспектов вероятностной оценки угроз НСД объектов КИИ в рамках методического аппарата уже достаточно хорошо зарекомендовавшей себя на практике методики определения актуальных угроз безопасности информации, как это показано выше.

Второе обстоятельство связано с возможностью построения функциональных моделей угроз НСД на основе установленных закономерностей практики выявления инцидентов, связанных с реализацией такого рода угроз. Данный класс моделей позволяет детализировать последовательность действий нарушителя при реализации угрозы для достижения своих целей. В отличие от приведенного в Приложении 11 «Методики оценки угроз безопасности информации»[3] перечня основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, функциональные модели угроз НСД к информации отражают уже сложившиеся взгляды специалистов относительно сценариев их реализации. Это является основанием для отказа от процедуры экспертной оценки вариантов построения сценариев реализации угроз в пользу их однотипного функционального представления, детализированного с учетом возможных условий их реализации. При этом за основу целесообразно взять официально установленное руководящими документами ФСТЭК России функциональное представление такого рода угроз.

Кроме того, следует учитывать, что функциональная модель угрозы НСД объекта КИИ, кроме способа детализированного представления выполняемых действий нарушителя по реализации угрозы, является инструментом ее формализованного представления. Это позволяет разрабатывать на его основе математические модели временных характеристик угрозы. В свою очередь такие модели позволяют решить и

обозначенную выше проблему учета случайных состояний, характеризующих моменты времени возникновения угроз и моменты времени их обнаружения соответствующими средствами защиты информации, т.е. учета случайных состояний, характеризующих динамику угрозы на фоне процессов реагирования на ее проявление [9].

2. Алгоритм построения функциональной модели угрозы НСД к информации объектов критической информационной инфраструктуры

В соответствии с общеметодологическим подходом [10] алгоритм разработки функциональной модели реализуется в два этапа.

На первом этапе путем детализации целевой функции исследуемого процесса образуются уровни ее функциональной декомпозиции. В случае, когда функциональное моделирование используется в качестве инструмента первичной формализации, уровень детализации считается достаточным, если на основе выделяемых функциональных компонент образуется функциональное представление, описываемое в терминах марковских процессов [11].

На втором этапе путем эмпирического исследования взаимосвязи между функциональными компонентами на каждом из уровней декомпозиции целевой функции устанавливается порядок их реализации (выполнения).

При реализации первого этапа построения функциональной модели угроз НСД на объектах КИИ воспользуемся предложенным в руководящих документах ФСТЭК России вариантом функционального представления такого рода угроз и группирования их функциональных компонент (рис. 1). При этом классификационными основаниями будем считать: стратегию реализации угрозы (С), используемые при этом тактики (Т), этапы действий нарушителя (Э), а также выполняемые им процедуры доступа к операционной среде КС и деструктивного воздействия на информацию (П).

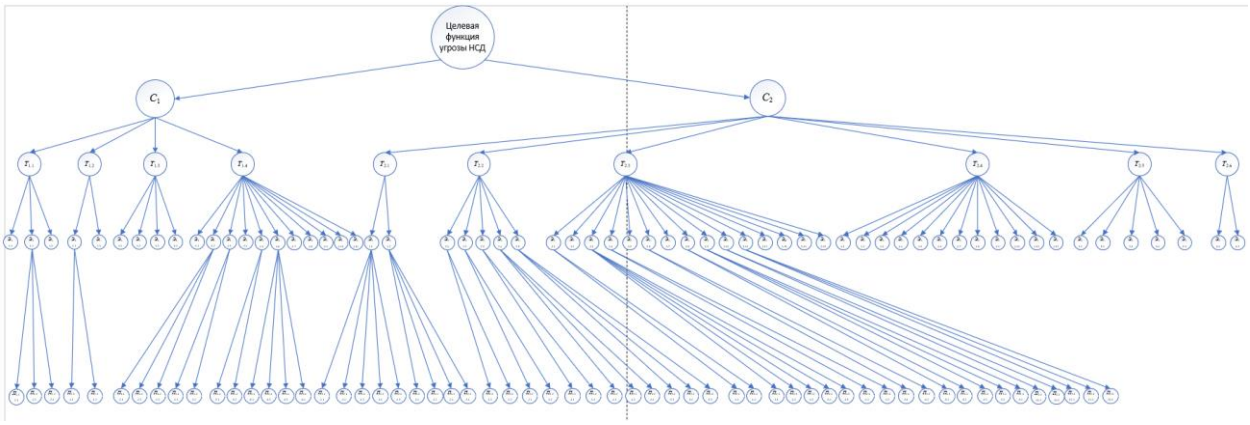

Рис. 1. Детализация целевой функции угрозы НСД к информации объектов КИИ
Fig. 1. Detailing the target function of the threat of unauthorized access to the information of CII objects

В соответствии со вторым этапом устанавливается порядок реализации функциональных компонент на каждом из представленных уровней. При идентификации этих компонент будем использовать терминологию функционального представления такого рода угроз, установленную руководящими документами ФСТЭК России.

На рис. 2 представлен порядок реализации целевой функции *Ц* – «Угроза НСД к информации объекта КИИ» соответствующими функциональными компонентами (стратегиями):

C_1 – «Непосредственный доступ к информации объекта КИИ»;

C_2 – «Удаленный доступ к информации объекта КИИ».

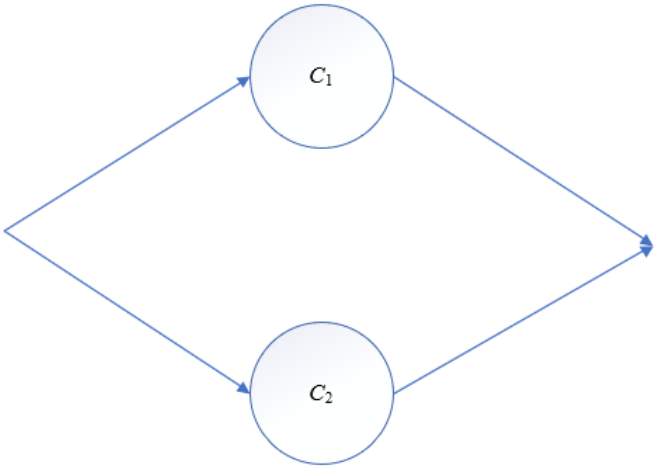

Рис. 2. Функциональное представление целевой функции «Угроза НСД к информации объекта КИИ»
Fig. 2. Functional representation of the objective function «Threat of unauthorized access to the information of a CII object»

На рис. 3 приводится порядок реализации стратегии C_1 – «Непосредственный доступ к информации объекта КИИ» соответствующими функциональными компонентами (тактиками):

$T_{1.1}$ – «Непосредственный доступ в процессе запуска операционной системы (ОС)»;

$T_{1.2}$ – «Непосредственный доступ к ОС»;

$T_{1.3}$ – «Непосредственный доступ к включенному компьютеру с загруженной ОС, но заблокированному»;

$T_{1.4}$ – «Непосредственный доступ к включенному компьютеру с загруженной ОС».

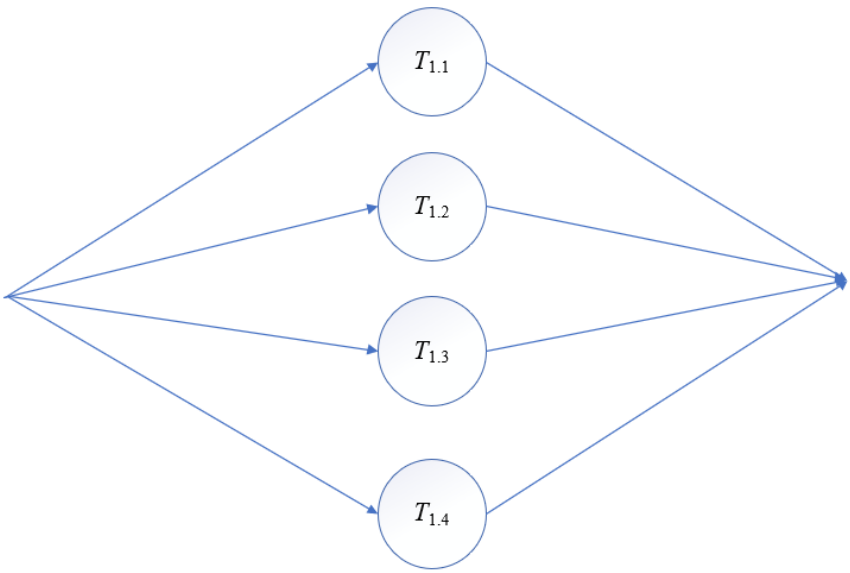

Рис. 3. Функциональное представление стратегии C_1 – «Непосредственный доступ к информации объекта КИИ»
Fig. 3. Functional representation of strategy C1 – «Direct access to information of a CII object»

Функциональными компонентами (тактиками), реализующими стратегию C_2 – «Удаленный доступ к информации объекта КИИ», являются:

$T_{2.1}$ – «Действия по подготовке к удаленной атаке»;
$T_{2.2}$ – «Попытка доступа к удаленному компьютеру»;
$T_{2.3}$ – «Доступ к удаленному компьютеру»;
$T_{2.4}$ – «Атаки на пользователей Internet»;
$T_{2.5}$ – «Отказ в обслуживании (DoS)»;
$T_{2.6}$ – «Атаки на МСЭ».

Порядок реализации этих тактик приводится на рис. 4.

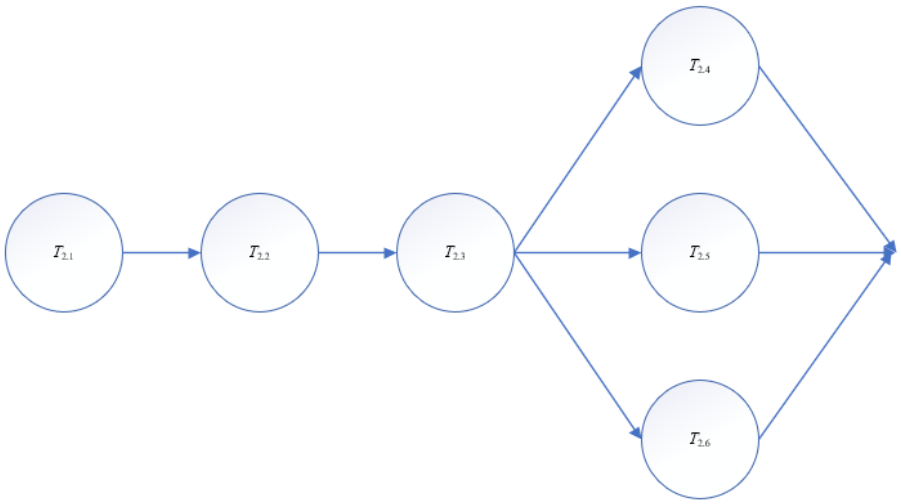

Рис. 4. Функциональное представление стратегии C_2 – «Удаленный доступ к информации объекта КИИ»
Fig. 4. Functional representation of strategy C2 – «Remote access to information of a CII object»

Функциональными компонентами, реализующими тактики, являются этапы. В качестве примера на рис. 5 приводится порядок реализации тактики $T_{2.3}$ – «Доступ к удаленному компьютеру»:

этап $Э_{2.3.1}$ – «Анализ информации, доступной после осуществления доступа к компьютеру»;
этап $Э_{2.3.2}$ – «Переполнение буфера с запуском исполняемого кода»;
этап $Э_{2.3.3}$ – «Инсталляция программного обеспечения (ПО) с последующим запуском»;
этап $Э_{2.3.4}$ – «Выявление пароля доступа в ОС»;
этап $Э_{2.3.5}$ – «Подмена системного ПО»;
этап $Э_{2.3.6}$ – «Создание новой учетной записи с расширенными привилегиями»;
этап $Э_{2.3.7}$ – «Уничтожение системного реестра»;
этап $Э_{2.3.8}$ – «Редактирование системного реестра»;
этап $Э_{2.3.9}$ – «Перехват внутрисегментного сетевого трафика»;
этап $Э_{2.3.10}$ – «Перенаправление сетевого трафика»;
этап $Э_{2.3.11}$ – «Внедрение ложного доверенного объекта»;
этап $Э_{2.3.12}$ – «Копирование информации на нештатные носители информации»;
этап $Э_{2.3.13}$ – «Модификация информации»;
этап $Э_{2.3.14}$ – «Уничтожение информации»;
этап $Э_{2.3.15}$ – «Форматирование носителей информации».

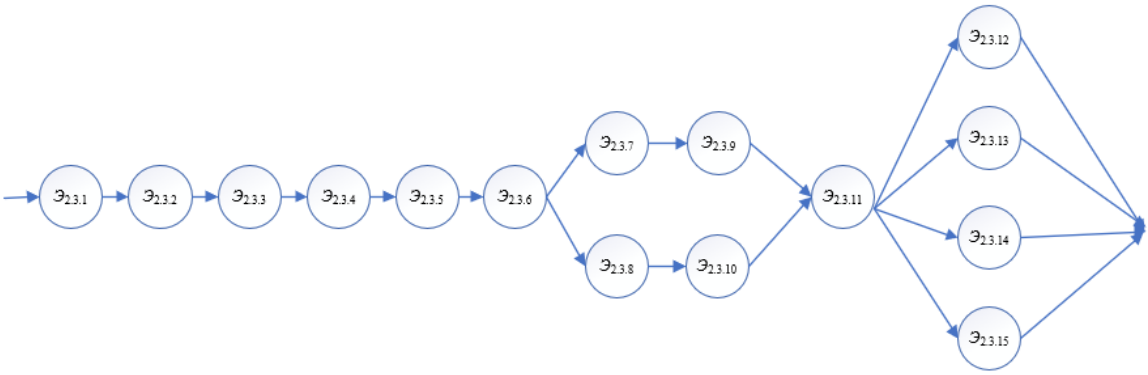

Рис. 5. Функциональное представление тактики $Т_{2.3}$ – «Доступ к удаленному компьютеру»
Fig. 5. Functional representation of tactics T2.3 – «Access to a remote computer»

Функциональными компонентами, реализующими этапы, являются выполняемые нарушителем процедуры. В качестве примера на рис. 6 приводится порядок реализации этапа $Э_{2.3.3}$ – «Инсталляция ПО с последующим запуском» функциональными компонентами (процедурами):

$П_{2.3.3.1}$ – «Инсталляция ПО «шпионом клавиатуры»»;
$П_{2.3.3.2}$ – «Инсталляция ПО, расширяющего привилегии пользователя»;
$П_{2.3.3.3}$ – «Инсталляция ПО, разрушающего аппаратное обеспечение компьютера»;
$П_{2.3.3.4}$ – «Инсталляция и запуск вируса»;
$П_{2.3.3.5}$ – «Инсталляция программ удаленного управления».

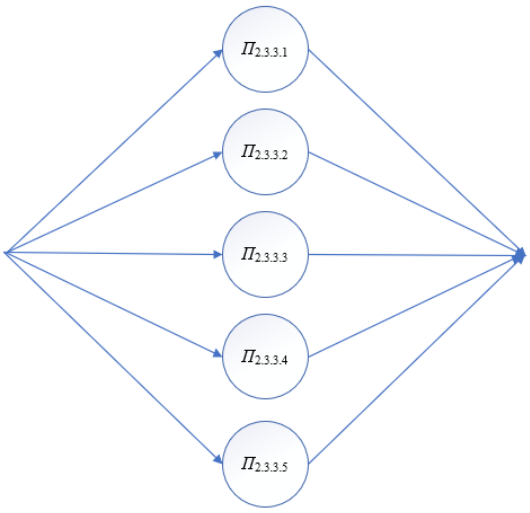

Рис. 6. Функциональное представление этапа $Э_{2.3.3}$ – «Инсталляция ПО с последующим запуском»
Fig. 6. Functional representation of stage E2.3.3 – «Installation of software with subsequent launch»

3. Построение математических выражений, для оценки средних значений времени реализации функциональных компонент угрозы НСД к информации объекта КИИ

Полученные результаты декомпозиции функционального описания целевой функции угрозы НСД к информации объектов 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 процедур и временем выполнения этапов, реализующих эти процедуры;

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

временем выполнения тактик и временем выполнения стратегий, реализующих эти тактики;

временем выполнения стратегий 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 угрозы НСД к информации объектов КИИ воспользуемся свойством линейности и аддитивности, математического ожидания композиции случайных величин [12]. При этом для композиции случайных величин $\tau(\Phi_1)$, $\tau(\Phi_2)$, …, $\tau(\Phi_N)$, характеризующих время реализации последовательности функциональных компонент Φ_1, Φ_2, …, Φ_N, воспользуемся выражением:

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

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

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

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

В случае, когда функциональные компоненты Φ_1, Φ_2, …, Φ_K, связаны параллельно, для композиции случайных величин $\tau(\Phi_1)$, $\tau(\Phi_2)$, …, $\tau(\Phi_K)$, характеризующих время их реализации, будем использовать выражение:

$$\overline{\tau}(\Phi^{(+1)}) = \sum_{k=1}^{K} p(\Phi_k) \cdot \bar{\tau}\,(\Phi_k), \qquad (2)$$

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 угрозы НСД к информации объектов КИИ.

В качестве примера будем использовать проиллюстрированные выше функциональные компоненты.

Выражение (3), полученное в соответствии с приведенным на рис. 6 функциональным представлением этапа $Э_{2.3.3}$ – «Инсталляция ПО с последующим запуском», является выражением для определения среднего значения случайной величины времени $\tau(Э_{2.3.3})$, затрачиваемого нарушителем на реализацию данного этапа:

$$\overline{\tau}(Э_{2.3.3}) = p(П_{2.3.3.1}) \cdot \overline{\tau}(П_{2.3.3.1}) + p(П_{2.3.3.2}) \cdot \overline{\tau}(П_{2.3.3.2}) + + p(П_{2.3.3.3}) \cdot \overline{\tau}(П_{2.3.3.3}) + p(П_{2.3.3.4}) \cdot \overline{\tau}(П_{2.3.3.4}) + + p(П_{2.3.3.5}) \cdot \overline{\tau}(П_{2.3.3.5}), \qquad (3)$$

где $p(П_{2.3.3.1})$ и $\overline{\tau}(П_{2.3.3.1})$ – вероятность выполнения и среднее значение времени реализации процедуры $П_{2.3.3.1}$ – «Инсталляция ПО «шпион клавиатуры», соответственно;

$p(П_{2.3.3.2})$ и $\overline{\tau}(П_{2.3.3.2})$ – вероятность выполнения и среднее значение времени реализации процедуры $П_{2.3.3.2}$ – «Инсталляция ПО, расширяющего привилегии пользователя», соответственно;

$p(П_{2.3.3.3})$ и $\overline{\tau}(П_{2.3.3.3})$ – вероятность выполнения и среднее значение времени реализации процедуры $П_{2.3.3.3}$ – «Инсталляция ПО, разрушающего аппаратное обеспечение компьютера», соответственно;

$p(П_{2.3.3.4})$ и $\overline{\tau}(П_{2.3.3.4})$ – вероятность выполнения и среднее значение времени реализации процедуры $П_{2.3.3.4}$ – «Инсталляция и запуск вируса», соответственно;

$p(П_{2.3.3.5})$ и $\overline{\tau}(П_{2.3.3.5})$ – вероятность выполнения и среднее значение времени реализации процедуры $П_{2.3.3.5}$ – «Инсталляция программ удаленного управления», соответственно.

Выражение (4), полученное в соответствии с приведенным на рис. 5 функциональным представлением тактики $T_{2.3}$ - «Доступ к удаленному компьютеру», является выражением для определения среднего значения случайной величины времени $\tau(T_{2.3})$, затрачиваемого нарушителем на реализацию данной тактики:

$$\tau(T_{2.3})= \overline{\tau}(Э_{2.3.1}) + \overline{\tau}(Э_{2.3.2})+ \overline{\tau}(Э_{2.3.3}) + \overline{\tau}(Э_{2.3.4}) + \overline{\tau}(Э_{2.3.5})+ \overline{\tau}(Э_{2.3.6}) +(p(Э_{2.3.7}) (\overline{\tau}(Э_{2.3.7}) + \overline{\tau}(Э_{2.3.9})) + p(Э_{2.3.8}) (\overline{\tau}(Э_{2.3.8}) + \overline{\tau}(Э_{2.3.10}))) + \overline{\tau}(Э_{2.3.11}) + +(p(Э_{2.3.12}) \cdot \overline{\tau}(Э_{2.3.12}) + p(Э_{2.3.13}) \cdot \overline{\tau}(Э_{2.3.13}) + p(Э_{2.3.14}) \cdot \overline{\tau}(Э_{2.3.14}) + + p(Э_{2.3.15}) \cdot \overline{\tau}(Э_{2.3.15})), \quad (4)$$

где $\overline{\tau}(Э_{2.3.1})$ – среднее значение времени реализации этапа $Э_{2.3.1}$ – «Анализ информации, доступной после осуществления доступа к компьютеру»;

$\overline{\tau}(Э_{2.3.2})$ – среднее значение времени реализации этапа $Э_{2.3.2}$ – «Переполнение буфера с запуском исполняемого кода»;

$\overline{\tau}(Э_{2.3.3})$ – среднее значение времени реализации этапа $Э_{2.3.3}$ – «Инсталляция ПО с последующим запуском»;

$\overline{\tau}(Э_{2.3.4})$ – среднее значение времени реализации этапа $Э_{2.3.4}$ – «Выявление пароля доступа в ОС»;

$\overline{\tau}(Э_{2.3.5})$ – среднее значение времени реализации этапа $Э_{2.3.5}$ – «Подмена системного ПО»;

$\overline{\tau}(Э_{2.3.6})$ – среднее значение времени реализации этапа $Э_{2.3.6}$ – «Создание новой учетной записи с расширенными привилегиями»;

$p(Э_{2.3.7})$ и $\overline{\tau}(Э_{2.3.7})$ – вероятность выполнения и среднее значение времени реализации процедуры $Э_{2.3.7}$ – «Уничтожение системного реестра», соответственно;

$p(Э_{2.3.8})$ и $\overline{\tau}(Э_{2.3.8})$ – вероятность выполнения и среднее значение времени реализации процедуры $Э_{2.3.8}$ – «Редактирование системного реестра», соответственно;

$\overline{\tau}(Э_{2.3.9})$ – среднее значение времени реализации этапа $Э_{2.3.9}$ – «Перехват внутрисегментного сетевого трафика»;

$\overline{\tau}(Э_{2.3.10})$ – среднее значение времени реализации этапа $Э_{2.3.10}$ – «Перенаправление сетевого трафика»;

$\overline{\tau}(Э_{2.3.11})$ – среднее значение времени реализации этапа $Э_{2.3.11}$ – «Внедрение ложного доверенного объекта»;

$p(Э_{2.3.12})$ и $\overline{\tau}(Э_{2.3.12})$ – вероятность выполнения и среднее значение времени реализации процедуры $Э_{2.3.12}$ – «Копирование информации на нештатные носители информации», соответственно;

$p(Э_{2.3.13})$ и $\overline{\tau}(Э_{2.3.13})$ – вероятность выполнения и среднее значение времени реализации процедуры $Э_{2.3.13}$ – «Модификация информации», соответственно;

$p(Э_{2.3.14})$ и $\overline{\tau}(Э_{2.3.14})$ – вероятность выполнения и среднее значение времени реализации процедуры $Э_{2.3.14}$ – «Уничтожение информации», соответственно;

$p(Э_{2.3.15})$ и $\overline{\tau}(Э_{2.3.15})$ – вероятность выполнения и среднее значение времени реализации процедуры $Э_{2.3.15}$ – «Форматирование носителей информации», соответственно.

Выражение (5), полученное в соответствии с приведенным на рис. 4 функциональным представлением стратегии C_2 – «Удаленный доступ к информации объекта КИИ», является выражением для определения среднего значения случайной величины времени $\tau(C_2)$, затрачиваемого нарушителем на реализацию данной тактики:

$$\tau(C_2)= \overline{\tau}(T_{2.1}) + \overline{\tau}(T_{2.2}) + \overline{\tau}(T_{2.3}) + (p(T_{2.4}) \cdot \overline{\tau}(T_{2.4})) + (p(T_{2.5}) \cdot \overline{\tau}(T_{2.5})) + (p(T_{2.6}) \cdot \overline{\tau}(T_{2.6})), \quad (5)$$

где $\overline{\tau}(T_{2.1})$ – среднее значение времени реализации тактики $T_{2.1}$ – «Действия по подготовке к удаленной атаке»;

$\overline{\tau}(T_{2.2})$ – среднее значение времени реализации тактики $T_{2.2}$ – «Попытка доступа к удаленному компьютеру»;

$\overline{\tau}(T_{2.3})$ – среднее значение времени реализации тактики $T_{2.3}$ – «Доступ к удаленному компьютеру»;

$p(T_{2.4})$ и $\overline{\tau}(T_{2.4})$ – вероятность выполнения и среднее значение времени реализации процедуры $T_{2.4}$ – «Атаки на пользователей Internet», соответственно;

$p(T_{2.5})$ и $\overline{\tau}(T_{2.5})$ – вероятность выполнения и среднее значение времени реализации процедуры $T_{2.5}$ – «Отказ в обслуживании», соответственно;

$p(T_{2.6})$ и $\overline{\tau}(T_{2.6})$ – вероятность выполнения и среднее значение времени реализации процедуры $T_{2.6}$ – «Атаки на МСЭ», соответственно.

Выражение (6), полученное в соответствии с приведенным на рис. 3 функциональным представлением стратегии C_1 – «Непосредственный доступ к информации объекта КИИ», является выражением для определения среднего значения случайной величины времени $\tau(C_1)$, затрачиваемого нарушителем на реализацию данной тактики:

$$\tau(C_1)= p(T_{1.1}) \cdot \overline{\tau}(T_{1.1})+ p(T_{1.2}) \cdot \overline{\tau}(T_{1.2})+ p(T_{1.3}) \cdot \overline{\tau}(T_{1.3})+ p(T_{1.4}) \cdot \overline{\tau}(T_{1.4}) \quad (6)$$

где $p(T_{1.1})$ и $\overline{\tau}(T_{1.1})$ – вероятность выполнения и среднее значение времени реализации процедуры $T_{1.1}$ – «Непосредственный доступ в процессе запуска ОС», соответственно;

$p(T_{1.2})$ и $\overline{\tau}(T_{1.2})$ – вероятность выполнения и среднее значение времени реализации процедуры $T_{1.2}$ – «Непосредственный доступ к ОС», соответственно;

$p(T_{1.3})$ и $\overline{\tau}(T_{1.3})$ – вероятность выполнения и среднее значение времени реализации процедуры $T_{1.3}$ – «Непосредственный доступ к включенному компьютеру с загруженной ОС, но заблокированному», соответственно;

$p(T_{1.4})$ и $\overline{\tau}(T_{1.4})$ – вероятность выполнения и среднее значение времени реализации процедуры $T_{1.4}$ – «Непосредственный доступ к включенному компьютеру с загруженной ОС», соответственно.

Выражение (7), полученное в соответствии с приведенным на рис. 2 функциональным представлением целевой функции «Угроза НСД к информации объекта КИИ», является выражением для определения среднего значения случайной величины времени τ, затрачиваемого нарушителем на реализацию угрозы данного типа:

$$\tau= p(C_1) \cdot \overline{\tau}(C_1)+ p(C_2) \cdot \overline{\tau}(C_2) \quad (7)$$

где $p(C_1)$ и $\overline{\tau}(C_1)$ – вероятность выполнения и среднее значение времени реализации процедуры C_1 – «Непосредственный доступ», соответственно;

$p(C_2)$ и $\overline{\tau}(C_2)$ – вероятность выполнения и среднее значение времени реализации процедуры C_2 – «Удаленный доступ», соответственно.

Заключение

Предложенный методический подход, основанный на использовании методологии функционального моделирования в качестве основания для разработки аналитических выражений временных характеристик функциональных компонент угроз НСД к информации КИИ дает возможность решения проблемы адекватной оценки такого рода угроз. Это позволяет, на основе разработанной оценки, обеспечить обоснованность требований к способам и средствам защиты информации от НСД в системах рассматриваемого класса.

СПИСОК ЛИТЕРАТУРЫ:

1. Актуальные аспекты информационной безопасности, под ред. О.Б. Макаревича: Монография. Таганрог: Издательство ТТИ ЮФУ, 2011. – 448 с.
2. Вихорев С.В., Сычев А.М. Диалоги о безопасности информации, или введение в основы построения систем обеспечения безопасности информации: Монография. М.: Медиа Группа «Авангард», 2015. – 640 с.
3. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография. Воронеж: Кварта, 2018. – 558 с. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_BIBL_A_012090330/ (дата обращения: 19.06.2023).
4. Сычев А.М., Вайц Е.В., Цой Р.А., Ушакова А.А., Скрыль К.С. Системология и модели оценки характеристик эффективности мер обеспечения безопасности электронного банкинга. Промышленные АСУ и контроллеры. 2019, № 3, с. 56–64. URL: https://elibrary.ru/item.asp?id=37096775 (дата обращения: 19.06.2023). – EDN VWGOFG.
5. Мазин А.В., Гайфулин В.В., Чудин К.С., Ходырев Т.Б., Тегенцев И.М. Теория информации как методологическая основа решения проблем адекватной оценки возможностей по обеспечению защиты информации. Известия Института инженерной физики. 2022, № 2(64), с. 64–68. URL: https://elibrary.ru/item.asp?id=48549191 (дата обращения: 19.06.2023). – EDN NXNGMV.
6. Скрыль Сергей В. и др. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. т. 28, № 1, с. 85–94, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.1.07. – EDN NOWDER.
7. Вайц Е.В., Сычев В.М. Методика оценки угроз безопасности информации ФСТЭК России как концепция исследования вопросов обеспечения безопасности объектов инфокоммуникационной инфраструктуры электронной коммерции. Вопросы защиты информации. 2021. № 4(135), с. 50–53. DOI: http://dx.doi.org/10.52190/2073-2600_2021_4_50.
8. Гайфулин В.В., Вайц Е.В., Сычев В.М. Методика оценки угроз безопасности ФСТЭК России как инструмент исследования киберустойчивости объектов информационной инфраструктуры. Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму: сборник трудов Всероссийской научно-практической конференции. Краснодар: Краснодарский университет МВД России. 2021, с. 20–24. – EDN MMQOGV.
9. Вайц Е.В., Сычев В.М. Математическое моделирование как инструмент обоснования требований к характеристикам мер обеспечения технологической устойчивости информационных систем розничных сетей. Вопросы защиты информации. 2021, № 3(144), с. 52–58. DOI: http://dx.doi.org/10.52190/2073-2600_2021_3_52. – EDN UGTTYU.
10. 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. URL: https://elibrary.ru/item.asp?id=35466900. – EDN ALESTB.
11. Тихонов В.И., Миронов М.А. Марковские процессы. М.: Сов. Радио, 1977. – 488 с.
12. Скрыль С.В., Сычев В.М., Мещерякова Т.В., Никитина Ю.С., Гайфулин В.В., Суворов А.А. Математические модели временных характеристик угроз несанкционированного доступа к компьютерной информации. Промышленные АСУ и контроллеры. 2019, № 11, с. 60–65. DOI: http://dx.doi.org/10.25791/asu.11.2019.999. – EDN PEUEDV.

REFERENCES:

[1] Current aspects of information security, edited by O.B. Makarevich: Monograph. Taganrog: Publishing house of TTI SFU, 2011. – 448 p. (in Russian).

[2] Vikhorev S.V., Sychev A.M. Dialogues on information security, or an introduction to the basics of building information security systems: Monograph. M.: Avangard Media Group, 2015. – 640 p. (in Russian).

[3] Yazov Y.K., Soloviev S.V. Organization of information protection in information systems from unauthorized access: monograph. Voronezh: Kvart, 2018. – 558 p. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_BIBL_A_012090330 (accessed: 19.06.2023) (in Russian).

[4] Sychev A.M., Vayts E.V., Tsoy R.A., Ushakova A.A., Skryl' K.S Systemology and model performance evaluation the effectiveness of security measures in electronic banking. Industrial automated control systems and controllers. 2019, no. 3, p. 56–64. URL: https://elibrary.ru/item.asp?id=37096775 (accessed: 19.06.2023) (in Russian). – EDN VWGOFG.

[5] Mazin A.V., Gaifulin V.V., Chudin K.S., Khodyrev T.B., Tegentsev I.M. Information theory as a methodological basis for solving problems of adequate assessment of information security capabilities. Proceedings of the Institute of Engineering Physics. 2022, no. 2 (64), p. 64–68. URL: https://elibrary.ru/item.asp?id=48549191. (accessed: 19.06.2023) (in Russian). – EDN NXNGMV.

[6] Skryl' Sergey V. et al. Topical issues of the problem of assessment of threats of cyber attacks on information resources of significant facilities of critical information infrastructure. IT Security (Russia), [S.l.], v. 28, no. 1, p. 84–94, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.1.07 (in Russian). – EDN NOWDER.

[7] Vaitc E.V., Sychev V.M. Methodology For Assessing Threats To Information Security By Fstec Of Russia As A Concept For Researching The Security Issues Of Objects Of The Infocommunication System Of E-Commerce. Information security issues. 2021, no. 4(135), p. 50–53. DOI: http://dx.doi.org/10.52190/2073-2600_2021_4_50 (in Russian). – EDN HMQQUM.

[8] Gaifullin V.V., Vaits E.V., Sychev V.M. Methodology for assessing security threats of the FSTEC of Russia as a tool for studying the cyber stability of information infrastructure facilities. Information and telecommunication technologies in countering extremism and terrorism: Proceedings of the All-Russian Scientific and Practical Conference. Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia. 2021, p. 20–24 (in Russian). – EDN MMQOGV.

[9] Vaitc E.V., Sychev V.M. Mathematical modeling as a tool for substantiating the requirements for the characteristics of measures to ensure the technological stability of information systems of retail chains. Information security issues. 2021, no. 3(144), p. 52–58. DOI: http://dx.doi.org/10.52190/2073-2600_2021_3_52 (in Russian). – EDN UGTTYU.

[10] Sychev A.M., Gayfulin V.V., Zelentsov V.V., Ponomarev M.V., Tegentsev I.M. The Main Theoretical Provisions Of The Assessment Methodology Characteristics Of Information Security Measures. Aerospace instrumentation. 2018, no. 8, p. 46–53. URL: https://elibrary.ru/item.asp?id=35466900 (in Russian). – EDN ALESTB.

[11] Tikhonov V.I., Mironov M.A. Markov processes. M.: Soviet Radio, 1977. – 488 p. (in Russian).

[12] Skryl S.V., Sychev V.M., Meshcheryakova T.V., Nikitina Yu.S., Gayfulin V.V., Suvorov A.A. Mathematical Models Of The Temporal Characteristics Of Threats Of Unauthorized Access To Computer Information. Industrial automated control systems and controllers. 2019, no. 11, p. 60–65. DOI: http://dx.doi.org/10.25791/asu.11.2019.999. – EDN PEUEDV.

Поступила в редакцию – 19 июля 2023 г. Окончательный вариант – 20 октября 2023 г.
Received – July 17, 2023. The final version – October 20, 2023.