УДК 004.891.1
DOI: 10.18469/ikt.2025.23.1.07

АНАЛИЗ ПОВЕДЕНИЯ ИНСАЙДЕРА В ИНФОРМАЦИОННОЙ СИСТЕМЕ В УСЛОВИЯХ ВЛИЯНИЯ ЗЛОУМЫШЛЕННИКА

Карпова Н.Е., Саранская А.А.
Самарский государственный технический университет, Самара, РФ
E-mail: esib@samgtu.ru

Статья посвящена исследованию поведения инсайдера в информационной системе под влиянием злоумышленника. Одним из наиболее серьезных видов угроз является взаимодействие внешних злоумышленников с инсайдерами. Внутренние пользователи, будучи частью организации, имеют доступ к критически важным данным и системам, что делает их привлекательной целью для злоумышленников. Для эффективного противодействия таким угрозам необходимо структурированное понимание процессов, которые лежат в основе взаимодействия злоумышленника и инсайдера. В работе описываются методы воздействия злоумышленника на пользователя. Проанализирована мотивация инсайдера, которую может использовать злоумышленник для достижения целей. На основе анализа составлена семантическая сеть, описывающая взаимодействие инсайдера и злоумышленника. На основании данных описаний была выполнена разработка сети Петри для моделирования взаимодействия злоумышленника, инсайдера и информационной системы.

Ключевые слова: *информационная безопасность, поведение пользователя, инсайдер, злоумышленник, сети Петри, семантическая сеть, угрозы*

Введение и постановка задачи

В современных условиях цифровой трансформации и роста киберугроз, выявление аномальных действий пользователей в информационных системах становится одной из ключевых задач для обеспечения информационной безопасности организаций. По данным анонимного опроса InfoWatch, 51% утечек информации происходит по вине сотрудников – в результате неаккуратности, беспечности или умышленных действий [1]. Это подчеркивает необходимость внедрения и развития эффективных механизмов мониторинга и анализа поведения пользователей. Традиционные методы защиты, такие как антивирусы, брандмауэры и системы предотвращения вторжений хотя и остаются важными элементами информационной безопасности, часто недостаточно эффективны для обнаружения внутренних угроз. Внутренние злоумышленники могут использовать легитимные учетные записи и доступ к корпоративным ресурсам, что затрудняет их выявление через стандартные технические средства защиты. В таких случаях особую значимость приобретают технологии анализа поведения пользователей, которые позволяют оценивать действия пользователей [2].

Мониторинг безопасности информационной среды требует анализа всех видов угроз, однако если естественные факторы достаточно просто формализируются в плане рисков и защита от них достаточно понятна, то на угрозы, имеющие причиной человеческий фактор, необходимо обратить особое внимание, так как невозможно предсказать действия человека даже при том условии, что он не намерен причинить вреда. Сложности, с которыми сталкиваются разработчики моделей, связаны с тем, что все методы касаются описания поведения человека, которое плохо поддается формализации [3]. Эти сложности обусловлены как природой человеческого поведения, так и особенностями информационных систем. Так, некоторые действия пользователя могут быть интерпретированы как аномальные, хотя на самом деле они обусловлены какими-то обстоятельствами, например, срочная задача или ошибка.

На сегодняшний день существуют различные подходы к анализу поведения пользователей. Статистические методы основываются на сравнении текущих действий пользователя с его профилем. Методы машинного обучения используют алгоритмы классификации и кластеризации для автоматического выявления аномалий, что делает их более гибкими.

Организации все чаще и чаще сталкиваются с угрозами и инцидентами, возникшими вследствие действий пользователя. Так, например, по статистике компании Positive Technologies [4]

социальная инженерия остается одним из основных методов атаки на организации: этот метод использовался в каждой второй успешной атаке на организации (51%). Отметим, что в перечень атак, связанных с социальной инженерией, входит также и фишинг, подкуп, шантаж сотрудников, которые впоследствии могут выполнять неправомерные действия в информационной системе. Согласно отчету компании Solar Security за первый квартал 2024 года, 6% кибератак были связаны с компрометацией учетных записей сотрудников, 14% – с несанкционированным доступом к информационным системам. В обоих случаях угроза могла исходить от внутренних пользователей.

Стоит отметить, что часть данных инцидентов можно отследить при помощи выявления нестандартных действий пользователя в информационных системах [5].

Таким образом, в настоящее время актуальной задачей является выявление паттернов взаимодействия злоумышленника и инсайдера. Если пользователь начинает передавать данные внешним лицам или проявляет нехарактерное поведение, это может быть сигналом о потенциальной угрозе. Раннее обнаружение таких действий дает возможность предотвратить утечку данных, минимизировать ущерб и укрепить защиту.

В статье [6] предлагается использование сетей Петри для описания процессов обработки информации при функционировании элементов системы защиты объекта. Автор отмечает, что одним из достоинств сетей Петри является возможность строгого математического описания модели. Это позволяет проводить детальный анализ моделей систем защиты и более эффективно выстраивать систему управления информационной безопасностью.

В статье [7] рассмотрены различные Методы моделирования атак на графах. Автором описываются плюсы и минусы таких подходов как дерево атаки, сети Петри, Дерево неисправностей, дерево событий, дерево решений, граф атаки. Методы, основанные на графах, позволяют выстроить взаимосвязи между объектами и этапами атаки, подходят для многоступенчатых и комбинированных сценариев.

Статья [8] посвящена разработке и реализации системы обнаружения угроз в режиме реального времени с использованием байесовских сетей. Предложенная автором система демонстрирует высокую точность обнаружения угроз при низком уровне ложных срабатываний. Надежность предлагаемой модели основана на байесовских сетях для стохастических оценок в недетерминированных сценариях. Автором было доказано, что это достаточно удобный инструмент, который будет способствовать улучшению осведомленности о ситуации в информационной системе. Автор предполагает, что улучшить производительность предлагаемой модели, и вероятности можно в дальнейшем с использованием методов машинного обучения.

В [9] используются сети Байеса для обнаружения сетевых атак. Было проведено множество экспериментов, демонстрирующих, что предложенная модель выполняет обнаружение аномалий с повышенной частотой обнаружения и допустимой частотой ложных срабатываний. Введен новый алгоритм на основе наивного байесовского алгоритма для обнаружения атак в обучающих данных. Также разработан алгоритм для выявления DDos – атак.

Отслеживание взаимодействия злоумышленника и инсайдера – помогает предотвратить серьезные угрозы для организации. Инсайдеры имеют доступ к внутренним ресурсам и данным, что делает их потенциальной мишенью для злоумышленников. Злоумышленники могут использовать различные методы, такие как шантаж, подкуп или социальную инженерию, чтобы склонить инсайдера к сотрудничеству. Если такое взаимодействие остается незамеченным, злоумышленник может получить доступ к конфиденциальной информации, нарушить работу систем или даже нанести ущерб репутации компании. Важность отслеживания этих взаимодействий заключается в том, что оно позволяет выявить подозрительную активность на ранних этапах.

Исследование

Одним из наиболее серьезных видов угроз является взаимодействие внешних злоумышленников с внутренними сотрудниками (инсайдерами). Инсайдеры, будучи частью организации, имеют доступ к критически важным данным и системам, что делает их привлекательной целью для злоумышленников. Для эффективного противодействия таким угрозам необходимо структурированное понимание процессов, которые лежат в основе взаимодействия злоумышленника и инсайдера.

Взаимодействие злоумышленника, инсайдера и информационной системы представляет собой структурированную модель понятий, отношений и процессов, описывающих механизмы компрометации безопасности через внутренние угрозы.

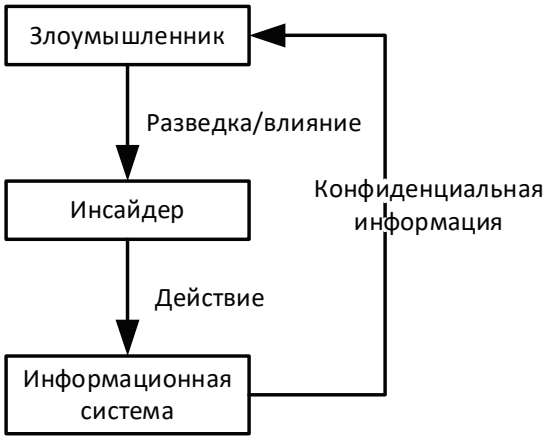

Рисунок 1. Структурные элементы взаимодействия

Структурные элементы взаимодействия представлены на рисунке 1. На первом этапе злоумышленник собирает информацию об инсайдере и системе. Злоумышленник может использовать информацию, которую пользователи выкладывают в открытых источниках и различные утечки информации, которые позволяют составить психологический портрет пользователя, его индивидуальные особенности, которые позволяют сделать атаку целевой [10]. Кроме того, злоумышленники могут использовать отчеты ведущих вендоров и регуляторов, в которых содержатся сведения о техниках и стратегиях действий злоумышленников, а также об ответных защитных мерах пользователей, что в дальнейшем может позволить злоумышленнику обойти эти меры. Злоумышленнику важно выявить возможную мотивацию пользователя к деструктивным действиям. Кроме того, понимание мотивации пользователей играет ключевую роль для специалистов по информационной безопасности. На основе этих данных они могут разрабатывать эффективные превентивные меры, направленные на нейтрализацию потенциальных рисков. Приведем пирамиду мотивации инсайдера (по аналогии с пирамидой Маслоу) (рисунок 2) [11].

Пирамида мотивации инсайдеров дает организациям системное понимание природы внутренних угроз, показывая, как базовые человеческие потребности и сложные психологические факторы могут трансформироваться в риски информационной безопасности. Чем ниже уровень – тем более базовые и распространенные мотивы. Чем выше – тем сложнее и целенаправленнее действия злоумышленника. Практическая ценность модели заключается в ее адаптивности – она дает возможность разрабатывать многослойную защиту, где технические контрмеры дополняются психологическим мониторингом и корпоративной культурой безопасности. При этом важно понимать, что верхние уровни пирамиды представляют наибольшую опасность, так как такие инсайдеры действуют осознанно, используя свои привилегии и знания систем.

Рисунок 2. Пирамида мотивации инсайдера

На основании собранных данных злоумышленник применяет различные методы для манипуляции инсайдером, после чего инсайдер выполняет деструктивные действия в отношении информационный системы. В итоге злоумышленник получает желаемый результат (доступ, данные, деньги). Информация циркулирует от Злоумышленника (Нарушителя) через Пользователя (Инсайдера) и обратно к нарушителю. Отметим, что каждый сотрудник имеет разную мотивацию к тому, чтобы стать инсайдером. Понимание того, что движет инсайдером, позволяет создать условия, при которых такие мотивы становятся менее значимыми.

Для визуализации взаимодействия злоумышленника, инсайдера и его доступа к информационным ресурсам удобно использовать семантическую сеть (рисунок 3). Семантическая сеть – информационная модель предметной области, имеет вид ориентированного графа. Вершины графа соответствуют объектам предметной области, а дуги (ребра) задают отношения между ними.

Семантическая сеть подчеркивает, что инсайдер является ключевым участником процесса, совершающим деструктивные действия под влиянием злоумышленника. Это позволяет более точно отразить роли и взаимодействия в системе, что важно для анализа угроз и разработки мер противодействия.

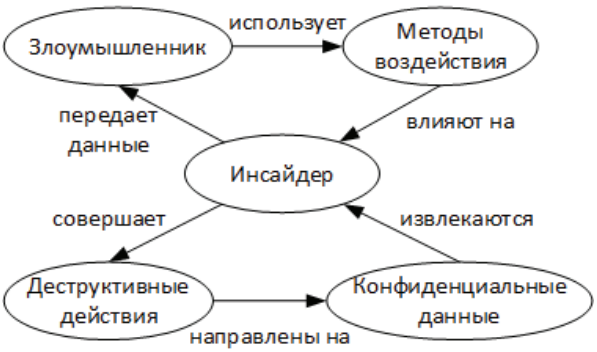

Рисунок 3. Семантическая сеть взаимодействия инсайдера и злоумышленника

На основании данных описаний была выполнена разработка сети Петри для моделирования взаимодействия злоумышленника-инсайдера и информационной системы. Сеть Петри требует учета различных состояний системы, действий злоумышленника и возможных последствий. Сеть Петри – ориентированный мультиграф, состоящий из вершин двух типов – позиций и переходов, соединенных между собой дугами. Вершины одного типа не могут быть соединены непосредственно. В позициях могут размещаться метки (маркеры), способные перемещаться по сети. Событием называют срабатывание перехода, при котором метки из входных позиций этого перехода перемещаются в выходные позиции. События происходят мгновенно либо разновременно, при выполнении некоторых условий [12]. В самом общем случае сетью Петри называется совокупность множеств:

$$C = \{P, T, I, O\}, \qquad (1)$$

где P – конечное множество, элементы которого называются позициями;

T – конечное множество, элементы которого называются переходами;

I – множество входных функций;

O – множество выходных функций.

На рисунке 4 обозначены p1 – злоумышленник активен, t1 – найти инсайдера, p2 – инсайдер найден, t2 – отправить фишинговое письмо, t3 – предложить инсайдеру финансовую выгоду, t4 – надавить на проблемные места инсайдера в компании, t5 – притвориться руководителем, p3 – инсайдер вовлечен, t6 – получить доступ к системе, p4 – доступ к системе есть, t7 – получить доступ к конфиденциальным данным, p5 – данные доступны, t8 – выкачивать данные из системы, t9 – зашифровать данные, t10 – подменить данные, t11 – уничтожить данные, p6 – данные выкачаны, t12 – передать данные злоумышленнику, p10 – данные переданы, p7 – данные зашифрованы, p8 – данные подменены, p9 – данные уничтожены.

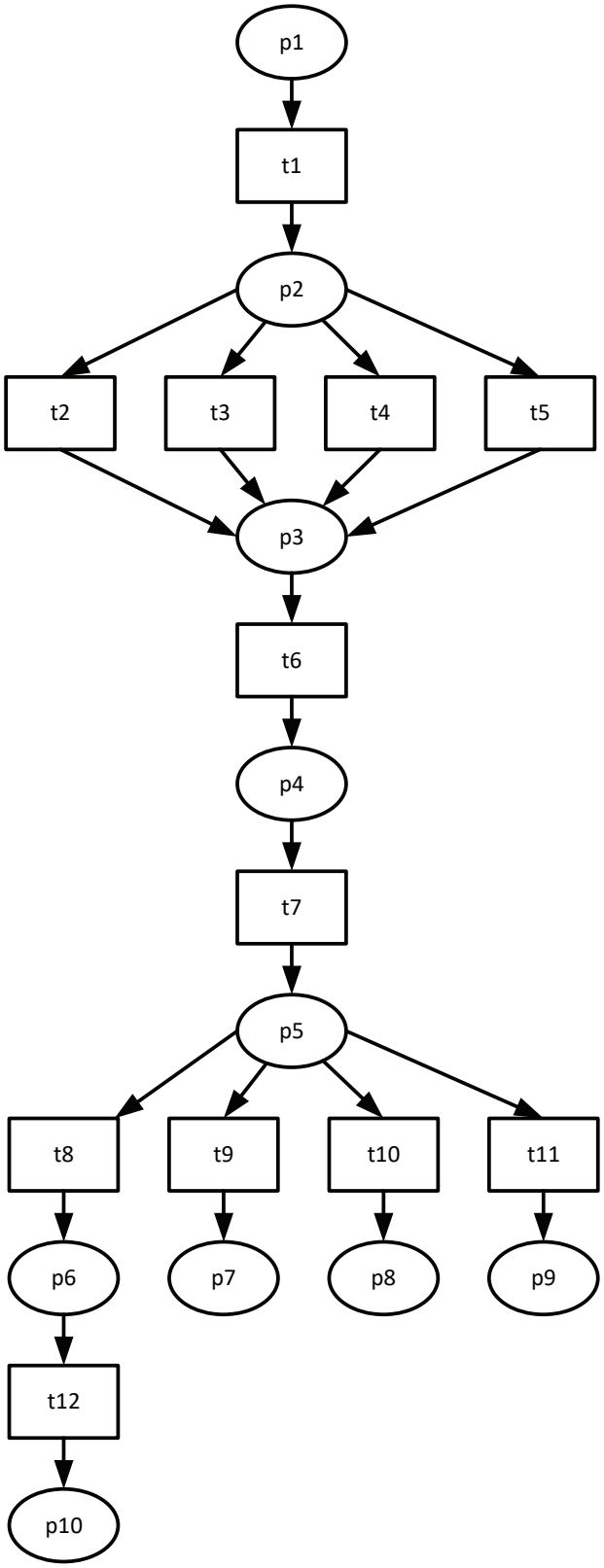

Рисунок 4. Сеть Петри для моделирования взаимодействия злоумышленника-инсайдера и информационной системы

Заметим, что преимущество использования сетей Петри состоит в том, что данную сеть можно преобразовать в блок-схему. Данный алгоритм ложится в основу системы по выявлению атак, свя-

занных с инсайдером. Все переходы из состояния в состояние связаны с продвижением злоумышленника к конфиденциальным данным, что приводит к инцидентам информационной системы.

Другим подходом является представление сети как взвешенного ориентированного графа. Веса можно задать на основании статистических данных или с помощью метода экспертных оценок.

Данный подход будет обладать прогностическим свойством и позволит в режиме реального времени оценивать актуальную ситуацию в системе и реагировать на происходящие события.

Важной задачей является разработка системы, учитывающей не только действия пользователя, но и взаимодействие его с злоумышленником. Отметим, что для выявления изменений в поведении потенциального инсайдера существует комплекс показателей, охватывающих различные аспекты его деятельности. В психологическом аспекте следует обращать внимание на повышенную тревожность, нервозность или замкнутость сотрудника, неадекватные реакции на обычные рабочие ситуации, избегание контактов с коллегами. Социальные изменения могут проявляться во внезапной смене круга общения, установлении подозрительных контактов с бывшими сотрудниками или представителями конкурирующих организаций, а также в частом обсуждении финансовых проблем или недовольства руководством.

В цифровой сфере сигналами служат нехарактерные объемы передаваемых данных, подключение к нестандартным сетевым ресурсам, использование средств анонимизации, множественные неудачные попытки входа в систему, авторизация с необычных устройств или географических локаций.

Для выявления этих изменений используются различные инструменты, включая системы мониторинга активности пользователей и анализа поведения (DLP, SIEM, UEBA), средства биометрической аутентификации, психологические опросы и интервью, наблюдение со стороны HR-специалистов, анализ корпоративных коммуникаций. Современные интегрированные системы обнаружения могут включать поведенческие анализаторы с видеонаблюдением и оценкой мимики, датчики стресса, когнитивные системы анализа больших данных, а также организационные меры в виде программ поощрения за сообщение о подозрительной активности.

Заключение

В статье предложен анализ мотивации инсайдера, а также семантическая сеть и сеть, описывающая взаимодействие злоумышленника, инсайдера и информационной системы. На основе данного описания разработана сеть Петри. Отметим, что пользователь является ключевым элементом в информационной системе, однако стоит оценивать его действия в контексте воздействия на него злоумышленника. В таком случае мы получим наиболее эффективный мониторинг и возможность реагирования на инциденты на ранних стадиях.

Литература

1. Слив данных сотрудниками, кибератаки и мошенничество: как бизнесу справиться с рисками корпоративных коммуникаций // ComNews. URL: https://www.comnews.ru/content/237226/2025-02-06/2025-w06/1013/sliv-dannykh-sotrudnikami-kiberataki-i-moshennichestvo-kak-biznesu-spravitsya-riskami-korporativnykh-kommunikaciy (дата обращения: 06.02.2025).
2. Карпова Н.Е., Саранская А.А. Исследование действий пользователя в информационной системе // Решетневские чтения: материалы XXVIII Международной научно-практической конференции, посвященной 100-летию со Дня рождения генерального конструктора ракетно-космических систем академика Михаила Федоровича Решетнева. Красноярск: Сибирский государственный университет науки и технологий им. М.Ф. Решетнева, 2024. С. 50–57. DOI: 10.33764/2618-981X-2023-6-50-57
3. Development of the analyzing system for user's actions in the informational environment / N.E. Karpova [et al.] // Journal of Physics: Conference Series. 2021. Vol. 1791. DOI: 10.1088/1742-6596/1791/1/012047
4. Актуальные киберугрозы II квартал 2024 года // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-ii-kvartal-2024-goda/#id2 (дата обращения: 15.11.2024).
5. Кибератаки на российские компании во II квартале 2024 года // Solar. URL: https://rt-solar.ru/analytics/reports/4544/ (дата обращения: 10.02.2025).
6. Шрейдер М.Ю., Боровский А.С. Разработка моделей описания обработки информации в задачах управления системой защиты объекта на основе сетей Петри // Вопросы кибер-безопасности. 2018. № 1 (25). С. 46–53. DOI: 10.21681/2311-3456-2018-1-46-53
7. Методы моделирования атак на графах // Habr. URL: https://habr.com/ru/companies/pt/articles/861072/ (дата обращения: 15.01.2025).
8. Pappaterra M.J. Implementing Bayesian Networks for Online Threat Detection: Dissertation

or Thesis. Uppsala University, 2018. 100 p. DOI: 10.13140/RG.2.2.23699.63521
9. Thwaini M.H. Anomaly detection in network traffic using machine learning for early threat detection // Data & Metadata. 2022. Vol. 1. P. 34. DOI: 10.56294/dm202272
10. Karpova N.E., Zolotarev V.V., Zolotareva E.Y. Using user profiles for dynamic correction of phishing attack response scenarios // AISMA-2024: International Workshop on Advanced Information Security Management and Applications. Lecture Notes in Networks and Systems. Cham: Springer, 2024. Vol. 863. P. 106–114. DOI: 10.1007/978-3-031-72171-7_11
11. Маслоу А. Мотивация и личность / пер. с англ. 3-е изд. СПб.: Питер, 2019. 400 с.
12. Котов В.Е. Сети Петри. М.: Наука, 1984. 160 с.

Дата поступления 03.02.2025
Дата принятия 03.03.2025

Карпова Надежда Евгеньевна, к.т.н., заведующий кафедрой электронных систем и информационной безопасности (ЭСИБ) Самарского государственного технического университета (СамГТУ). 443100, г. Самара, ул. Молодогвардейская, 244. Тел. +7 846 337-15-77. E-mail: esib@samgtu.ru

Саранская Алина Анатольевна, аспирант кафедры ЭСИБ СамГТУ. 443100, г. Самара, ул. Молодогвардейская, 244 Тел. +7 846 337-15-77. E-mail: esib@samgtu.ru

UDC 004.891.1
DOI: 10.18469/ikt.2025.23.1.07

ANALYSIS OF INSIDER BEHAVIOR IN AN INFORMATION SYSTEM UNDER THE INFLUENCE OF AN INVADER

Karpova N.E, Saranskaya A.A.
Samara State Technical University, Samara, Russian Federation
E-mail: esib@samgtu.ru

The article is addressed to the study of insider behavior in an information system under the influence of an invader. One of the most serious types of threats is the interaction of external intruders with employees. Insiders, as a part of an organization, have access to critical data and systems, making them an attractive target for intruders. To effectively counter such threats, a structured understanding of the processes that underlie the interaction of an intruder and an insider is necessary. The article describes methods of invader's influence on an insider. The motivation of an insider, which can be used by an attacker to achieve goals, is analyzed. Based on the analysis, a semantic network was compiled describing the interaction of an insider and an intruder. Based on these descriptions, a Petri net was developed in order to create a model of the interaction of an intruder, an insider, and an information system.

Keywords: *information security, user behavior, insider, attacker, Petri nets, semantic network, threats*

Karpova Nadezhda Evgenievna, Samara State Technical University, 244, Molodogvardeyskaya Street, Samara, 443010, Russian Federation; Head of Electronic Systems and Information Security Department, PhD in Technical Sciences. Tel. + 7 846 337-15-77. E-mail: esib@samgtu.ru

Saranskaya Alina Anatolievna, Samara State Technical University, 244, Molodogvardeyskaya Street, Samara, 443010, Russian Federation; PhD Student of Electronic Systems and Information Security Department. Tel. + 7 846 337-15-77. E-mail: esib@samgtu.ru

References

1. Data leaks by employees, cyberattacks, and fraud: how businesses can manage risks in corporate communications. *ComNews*. URL: https://www.comnews.ru/content/237226/2025-02-06/2025-w06/1013/sliv-dannykh-sotrudnikami-kiberataki-i-moshennichestvo-kak-biznesu-spravitsya-riskami-korporativnykh-kommunikaciy (accessed: 06.02.2025). (In Russ.)

2. Karpova N.E., Saranskaya A.A. Research on user actions in the information system. *Reshetnevskie chteniya: materialy XXVIII Mezhdunarodnoj nauchno-prakticheskoj konferencii, posvyashchennoj 100-letiyu so Dnya rozhdeniya general'nogo konstruktora raketno-kosmicheskih sistem akademika Mihaila Fedorovicha Reshetneva*. Krasnoyarsk: Sibirskij gosudarstvennyj universitet nauki i tekhnologij im. M.F. Reshetneva, 2024, pp. 50–57. DOI: 10.33764/2618-981X-2023-6-50-57 (In Russ.)
3. Karpova N.E. et al. Development of the analyzing system for user's actions in the informational environment. *Journal of Physics: Conference Series*, 2021, vol. 1791. DOI: 10.1088/1742-6596/1791/1/012047
4. Current cyber threats in the second quarter of 2024. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-ii-kvartal-2024-goda/#id2 (accessed: 15.11.2024). (In Russ.)
5. Cyber-attacks on Russian companies in the second quarter of 2024. *Solar*. URL: https://rt-solar.ru/analytics/reports/4544/ (accessed: 10.02.2025). (In Russ.)
6. Shreider M.Y., Borovsky A.S. Development of models for describing information processing in tasks of managing an object's protection system based on Petri nets. *Voprosy kiberbezopasnosti*, 2018, no. 1 (25), pp. 46–53. DOI: 10.21681/2311-3456-2018-1-46-53 (In Russ.)
7. Methods for modeling attacks on graphs. *Habr*. URL: https://habr.com/ru/companies/pt/articles/861072/ (accessed: 15.01.2025). (In Russ.)
8. Pappaterra M.J. *Implementing Bayesian Networks for Online Threat Detection*. Uppsala University, 2018, 100 p. DOI: 10.13140/RG.2.2.23699.63521
9. Thwaini M.H. Anomaly detection in network traffic using machine learning for early threat detection. *Data & Metadata*, 2022, vol. 1, pp. 34. DOI: 10.56294/dm202272
10. Karpova N.E., Zolotarev V.V., Zolotareva E.Y. Using user profiles for dynamic correction of phishing attack response scenarios. *AISMA-2024: International Workshop on Advanced Information Security Management and Applications. Lecture Notes in Networks and Systems.* Cham: Springer, 2024, vol. 863, pp. 106–114. DOI: 10.1007/978-3-031-72171-7_11
11. Maslow A. *Motivation and personality.* Transl. From English. 3nd ed. Saint Petersburg: Piter, 2019, 400 p. (In Russ.)
12. Kotov V.E. *Petri Nets.* Moscow: Nauka, 1984, 160 p. (In Russ.)

Received 03.02.2025
Accepted 03.03.2025