Краткие сообщения
Brief reports

Краткое сообщение
УДК 002.5:004
DOI: 10.14529/ctcr230208

ВЕРОЯТНОСТНЫЙ ПОДХОД К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ЗАДАЧЕ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

***Л.А. Артюшина**, larisa-artusina@yandex.ru, https://orcid.org/0000-0001-5160-5294*
Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия

Аннотация. **Цель исследования:** оценка защищенности ИС в процессе идентификации пользователя по клавиатурному почерку. **Материалы и методы.** Изучение и анализ научных публикаций по проблеме оценки защищенности информационных систем позволили выявить наиболее эффективный подход к оценке защищенности информационной системы, основанный на моделировании атак. Метод, рассмотренный в статье, представляет собой комбинацию графического и вероятностного подходов к анализу возможных сценариев реализации угроз в информационных системах для случая идентификации пользователя. Графическое представление в виде деревьев атак мы использовали для моделирования возможных путей атакующих действий нарушителя, связанных между собой в соответствии с тем, в какой последовательности их может выполнять нарушитель. Вероятностный подход в случае идентификации пользователя был использован нами для оценки вероятности успешности атаки на актив по пути, указанному в соответствующем дереве атак, и эффективности предлагаемых контрмер. **Результаты.** Обозначена совокупность наиболее информативных параметров клавиатурного почерка, к которой мы отнесли время нажатия клавиши, паузы между нажатиями клавиш и скорость набора. Для этой совокупности определены возможные сценарии развития событий в процессе идентификации пользователя, а также случаи, когда необходимо принять контрмеры: совпадают все три значения параметра клавиатурного почерка, контрмеры не предусмотрены; совпадают любые два из трех значений параметра клавиатурного почерка, требуется предусмотреть контрмеры; не совпадают два из трех или все три значения параметра клавиатурного почерка, требуется предусмотреть контрмеры. С помощью дерева атак смоделированы возможные варианты путей атак и возможные сценарии развития событий в процессе идентификации пользователя. С использованием вероятностного подхода рассчитаны вероятность успешной атаки на актив по пути, указанному в дереве атак, и степень эффективности предлагаемых контрмер. **Заключение.** Представленный в статье расчет уровня защищенности информационной системы будет полезен разработчикам и исследователям в их практической и научной деятельности.

Ключевые слова: вероятностный подход, защита информации, клавиатурный почерк, деревья атак, оценка защищенности

Для цитирования: Артюшина Л.А. Вероятностный подход к оценке защищенности информационной системы в задаче идентификации пользователя по клавиатурному почерку // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2023. Т. 23, № 2. С. 93–101. DOI: 10.14529/ctcr230208

Brief report
DOI: 10.14529/ctcr230208

A PROBABILISTIC APPROACH TO ASSESSING THE SECURITY OF THE INFORMATION SYSTEM IN THE PROBLEM OF USER IDENTIFICATION BY KEYPAD HANDWRITING

***L.A. Artyushina**, larisa-artusina@yandex.ru, https://orcid.org/0000-0001-5160-5294*
Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia

Abstract. **The purpose of the study.** Assessment of IP security in the process of user identification by keyboard handwriting. Materials and methods. The study and analysis of scientific publications on the problem of assessing the security of information systems allowed us to identify the most effective approach to assessing the security of an information system based on attack modeling. The method considered in the article is a combination of graphical and probabilistic approaches to the analysis of possible scenarios for the implementation of threats in information systems for the case of user identification. We used a graphical representation in the form of attack trees to model possible ways of attacking actions of the violator, interconnected in accordance with the sequence in which they can be performed by the violator. The probabilistic approach in the case of user identification was used by us to assess the probability of success of an attack on an asset along the path indicated in the corresponding attack tree and the effectiveness of the proposed countermeasures. **Results.** The set of the most informative parameters of keyboard handwriting is indicated, to which we attributed: the time of pressing the key, the pauses between keystrokes and the speed of typing. For this set, possible scenarios for the development of events in the process of user identification are identified, as well as cases when it is necessary to take countermeasures: all three values of the keyboard handwriting parameter coincide, countermeasures are not provided; any two of the three values of the keyboard handwriting parameter are combined, countermeasures must be provided; two of the three or all three values of the keyboard handwriting parameter do not match, it is necessary to provide countermeasures. With the help of the attack tree, possible variants of attack paths and possible scenarios for the development of events in the process of user identification are modeled. Using a probabilistic approach, the probability of a successful attack on an asset along the path indicated in the attack tree and the degree of effectiveness of the proposed countermeasures are calculated. **Conclusion.** The calculation of the security level of the information system presented in the article will be useful to developers and researchers in their practical and scientific activities.

Keywords: probabilistic approach, information protection, keyboard handwriting, attack trees, security assessment

For citation: Artyushina L.A. A probabilistic approach to assessing the security of the information system in the problem of user identification by keypad handwriting. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2023;23(2):93–101. (In Russ.) DOI: 10.14529/ctcr230208

Введение

Задаче повышения уровня защищенности информационных систем (ИС) посвящено большое количество работ. Актуальность проблемы безопасности информации, циркулирующей в ИС, с каждым днем лишь возрастает [1–6].

Для повышения уровня защищенности ИС необходимо регулярно проводить ее оценку и анализ. Полученные результаты позволят оптимизировать управляющие воздействия, механизмы выявления нарушителей и построить адекватную систему защиты информации, циркулирующей в ИС.

Одним из наиболее эффективных подходов к оценке защищенности является подход, основанный на моделировании атак, позволяющий учесть как вероятность осуществления атак определенного типа, так и их успешность.

Одним из представлений, описывающим возможные действия нарушителя, являются деревья атак [1–6]. Узлы дерева атак могут быть представлены как возможные пути атакующих действий

нарушителя, связанные между собой в соответствии с тем, в какой последовательности их может выполнять нарушитель.

Введем необходимые рабочие определения.

Вслед за [7] в рамках тематики статьи под нарушителем будем понимать физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах. Под защищенностью ИС – комплекс организационных мер и программно-технических средств защиты от несанкционированного доступа к информации в ИС. Под контрмерами – меры, внедрение которых позволяет снизить вероятность того, что источник угрозы сможет воспользоваться уязвимостью ИС.

Цель работы: оценка защищенности ИС в процессе идентификации пользователя по клавиатурному почерку. Для достижения поставленной цели решались следующие **задачи:**

– определить:

- совокупность параметров клавиатурного почерка, которые будут использованы для оценки уровня защищенности ИС;
- возможные сценарии развития событий в процессе идентификации пользователя, а также случаи, когда необходимо принять контрмеры;
- возможные варианты путей атак для выбранных ценных активов ИС;

– предусмотреть комплекс контрмер для устранения атак;

– сформировать дерево атак;

– с использованием вероятностного подхода рассчитать:

- вероятность успешной атаки на актив по пути, указанному в дереве атак;
- степень эффективности предлагаемых контрмер.

1. Определение совокупности параметров клавиатурного почерка и возможных сценариев атак

Основываясь на результатах анализа научных публикаций по проблеме биометрической идентификации пользователя [8–11], представленных нами в работе [12], к параметрам, обладающим высокой степенью информативности, мы отнесли: время нажатия (p1), паузы между нажатиями (p2) и скорость набора (p3).

Для оценки защищенности ИС в задаче идентификации пользователя мы определили возможные сценарии развития событий в процессе идентификации пользователя, а также случаи, когда необходимо принять контрмеры:

– совпадают все три значения параметра клавиатурного почерка, контрмеры не предусмотрены;

– совпадают любые два из трех значений параметра клавиатурного почерка. Требуется предусмотреть контрмеры;

– не совпадают два из трех или все три значения параметра клавиатурного почерка. Требуется предусмотреть контрмеры.

2. Моделирование путей атак для выбранной совокупности параметров клавиатурного почерка

Процесс моделирования возможных путей атак на активы ИС рассмотрим на примере организации обучения по курсу дисциплины на платформе moodle. В данном случае ценным активом для нарушителя являются информационные ресурсы, а именно Банк заданий и ответов, База данных обучаемых и их оценок.

Цель атаки на актив – получить доступ к информации, ограниченный лишь правами обучаемого (G_0).

Конкретизируем возможные сценарии развития событий в процессе идентификации пользователя.

Цель атаки не может быть достигнута в случаях, если все три значения параметров клавиатурного почерка соответствуют эталону пользователя (и(p1;p2;p3=true)).

Цель атаки может быть достигнута в случае выполнения хотя бы одного из следующих усло-

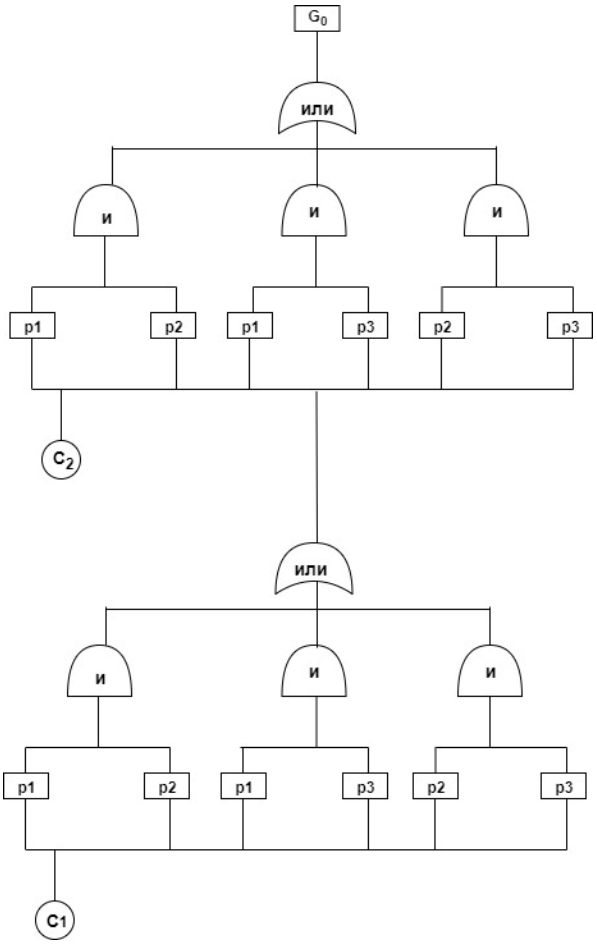

Рис. 1. Дерево атак с контрмерами для идентификации пользователя
Fig. 1. Attack tree with countermeasures for user identification

вий: время нажатия и паузы между нажатиями соответствуют эталону обучаемого, а скорость набора не соответствуют эталону обучаемого (и(p1;p2)=true, p3=false); время нажатия и скорость набора соответствуют эталону обучаемого, а паузы между нажатиями не соответствуют эталону обучаемого (и(p1;p3)=true, p2=false); время нажатия не соответствует эталону обучаемого, а паузы между нажатиями и скорость набора соответствуют эталону обучаемого (и(p2;p3)=true, p1=false).

Перечисленные условия образуют совокупность возможных путей атак на обозначенный актив ИС.

Для устранения атак нами были предусмотрены следующие контрмеры: в случае несоответствия одного из параметров эталону обучаемого необходимо предусмотреть дополнительную аутентификацию пользователя в виде ввода им контрольной фразы (c1), в случае повторного несоответствия одного из параметров эталону пользователя – отказать субъекту в доступе к ИС (c2).

Дерево атак, соответствующее сформулированным выше условиям, представлено на рис. 1.

3. Вероятностный подход к оценке рисков ИС

Вероятностный подход в случае идентификации [6, 13–15] пользователя был использован нами для оценки вероятности успешности атаки на актив по пути, указанному в соответствующем дереве атак, и эффективности предлагаемых контрмер.

Выделим основное событие (цель атаки – G_0). Варианты атак (базовые события): A – условие 1 – (и(p1;p2)=true, p3=false); B – условие 2 – (и(p1;p3)=true, p2=false); C – условие 3 – (и(p2;p3)=true, p1=false).

Рассчитаем вероятности базовых событий. Для этой цели обычно применяются: результаты тестирования ИС на атаки, экспертные оценки, известные статистические данные, опыт эксплуатации ИС и т. д. Мы использовали оценки эксперта. Использовалась трехбалльная шкала. Вероятности базовых событий определялись по формуле

$$P = w_1 \cdot u(S) + w_2 \cdot u(C) + w_3 \cdot u(L), \quad (1)$$

где w_1, w_2, w_3 – весовые коэффициенты, $\sum_1^3 w_i = 1$, $w_1 = w_2 = w_3 = 1/3$; S – сложность атаки (1 – реализация атаки не требует усилий, 2 – атаку просто реализовать, 3 – атака сложна в реализации), C – стоимость атаки (1 – атака низкой стоимости, 2 – атака средней стоимости, 3 – атака высокой стоимости), L – сложность обнаружения атаки (1 – атаку сложно обнаружить, 2 – атаку достаточно сложно обнаружить, 3 – атаку легко обнаружить). $u(x)$ – функция преобразования, вычисляемая по формуле

$$u(x) = \frac{c}{x}, \quad (2)$$

где c – коэффициент преобразования.

Коэффициент преобразования вычисляется экспериментальным путем. Значение, используемое в данном примере, вычислялось из допущения, что при минимальных оценках всех базовых событий (худший случай) вероятность основного события должна попадать под определение высокой вероятности успешной атаки. В данном случае использовалось значение $c = 0{,}3$.

Составим таблицу значений базовых событий (см. таблицу).

Значения базовых событий
Values of basic events

Имя базового события	S – сложность атаки	C – стоимость атаки	L – сложность обнаружения атаки
A	1	1	1
B	1	1	3
C	1	1	3

Уровень сложности обнаружения базового события A определен нами как низкий, так как из трех не совпадает параметр, наиболее зависящий от психологического (физического и т. п.) состояния пользователя, он менее стабилен, его легче как подделать, так и обнаружить.

Рассчитаем вероятности базовых событий по формуле (1):

$$P_{\text{A}} = \frac{1}{3}\cdot\frac{0{,}3}{1} + \frac{1}{3}\cdot\frac{0{,}3}{1} + \frac{1}{3}\cdot\frac{0{,}3}{1} = 0{,}3;$$

$$P_{\text{C}} = P_{\text{B}} = \frac{1}{3}\cdot\frac{0{,}3}{1} + \frac{1}{3}\cdot\frac{0{,}3}{1} + \frac{1}{3}\cdot\frac{0{,}3}{3} = 0{,}073,$$

где P_{A}, P_{B}, P_{C} – вероятности базовых событий A, B, C соответственно. Тогда дерево атак на первом этапе (без оценки эффективности контрмеры c1) будет выглядеть следующим образом (рис. 2).

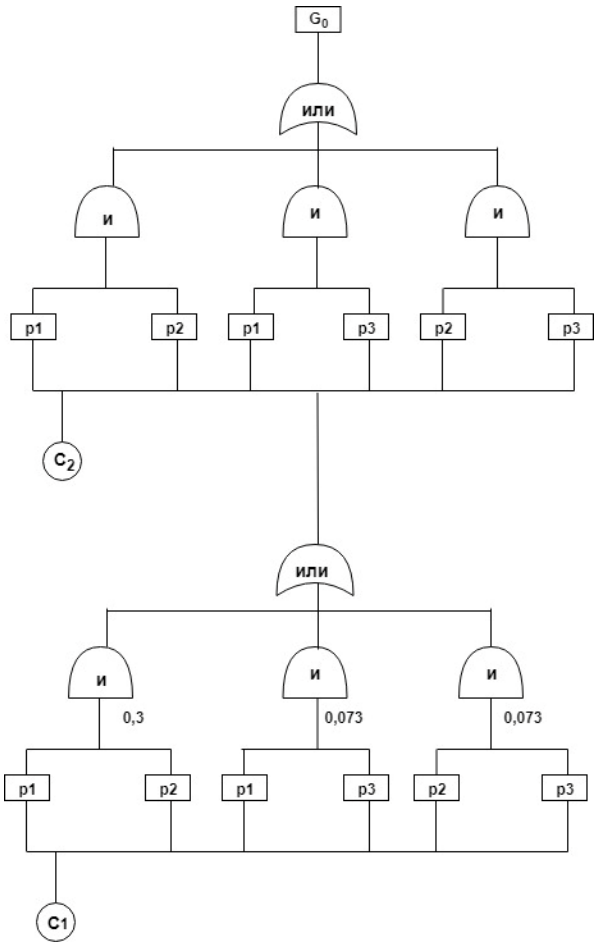

Рис. 2. Дерево атак на первом этапе оценки
Fig. 2. Attack tree at the first stage of evaluation

Далее рассчитывалась степень эффективности предлагаемых контрмер. Вероятность несанкционированного доступа к информации в условиях применения мер и средств защиты в компьютерной системе существенно зависит от того, где блокируется доступ к информации. У нас простой случай – на входе в ИС. В этом случае эффективность защиты информации только от несанкционированного доступа можно рассчитать по формуле

$$\eta(t) = 1 - P_{\text{acc}}(t)\cdot\max K, \qquad (3)$$

где $P_{\text{acc}}(t)$ – вероятность доступа нарушителя в ИС; $\max K$ – максимальный коэффициент опасности данной атаки.

Для базового события A: $P_{\text{acc}}(t) = 0{,}3$. Коэффициент опасности атаки вычислялся нами на основании баллов (дискретно от 1 до 10), выставленных экспертом по трем критериям (возможность возникновения источника угрозы ($K_1 = 10$), степень его готовности произвести атаку ($K_2 = 10$), а также фатальность для ИС от реализации атаки ($K_3 = 1$), по формуле

$$\max K = \frac{K_1 \cdot K_2 \cdot K_3}{10^3}. \qquad (4)$$

Получаем $\max K = 0{,}1$, тогда $\eta(t)_{\text{A}} = 1 - 0{,}3\cdot 0{,}1 = 0{,}97$.

Тогда вероятность прохождения нарушителя ($P_{\text{нар}}$) к следующему узлу дерева атак составит для случая А: $P_{\text{нар}} = 1 - 0,97 = 0,03$.

Эффективность контрмеры C_1 для события А – высокая.

Для базовых событий В и С:

$P_{\text{acc}}(t) = 0,073;\ \eta(t)_{\text{A}} = 1 - 0,073 \cdot 0,1 = 0,99.$

Тогда вероятность прохождения нарушителя к следующему узлу дерева атак составит для случаев А и В: $P_{\text{нар}} = 1 - 0,99 = 0,01$.

Эффективность контрмеры C_1 для событий В и С – высокая.

Дерево атак с учетом оценки эффективности контрмеры C_1 будет выглядеть следующим образом (рис. 3).

Аналогичным образом оценивалась эффективность применения контрмеры C_2. P_{A}, P_{B}, P_{C} соответственно равны 0,02, 0,01 и 0,01. Эффективность применения контрмеры C_2 для событий А, В, С составила 0,98 и 0,99, 0,99 соответственно. Дерево атак на завершающем этапе оценки представлено на рис. 4.

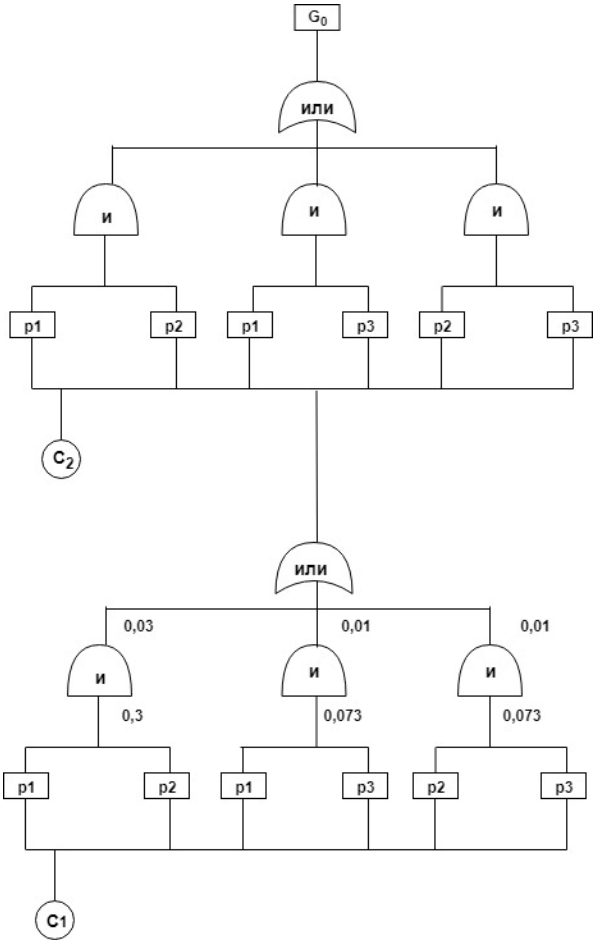

Рис. 3. Дерево атак на втором этапе оценки
Fig. 3. Attack tree at the second stage of evaluation

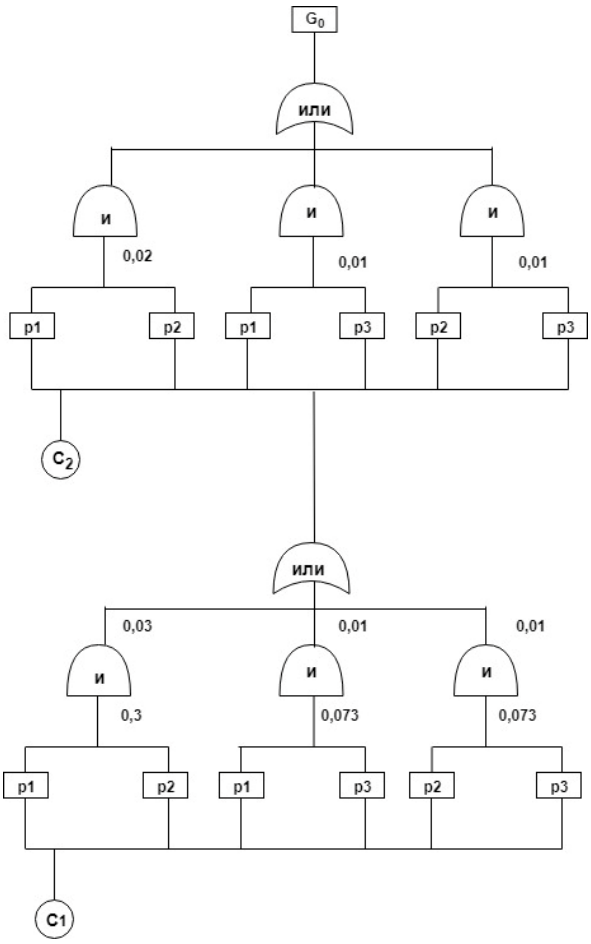

Рис. 4. Дерево атак на завершающем этапе оценки
Fig. 4. Attack tree at the final stage of evaluation

Заключение

В статье рассмотрена методика применения вероятностного подхода для оценки вероятности успешности атаки на актив ИС и эффективности предлагаемых контрмер.

Рассмотренная в рамках статьи методика анализа защищенности используется при проведении научно-исследовательских работ магистрантами Владимирского государственного университета, занимающимися проблемой оценки защищенности ИС.

Направление дальнейших исследований заключаются в исследовании способов уменьшения вероятности успешной атаки и создании метода автоматизированного выбора контрмер.

Таким образом, исследуемая проблема многоаспектна и не может быть исчерпана настоящей работой. Требуются объединенные усилия ученых различных профилей для рассмотрения как можно большего количества связей и отношений в ней.

Работа выполнена во Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых.

Список литературы

1. Алпеев Е.В., Стадник А.Н., Скрыль С.В. Методика прогнозирования компьютерных атак на основе определения весов атрибутов компьютерной атаки с применением метода деревьев решений // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2021. № 6. С. 82–92. ISSN: 2306-1456.

2. Кляус Т.К., Гатчин Ю.А. Определение вероятности реализации атак на информационную систему с помощью деревьев событий // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4 (30). С. 31–37. DOI: 10.14529/secur180405, ISSN: 2225-5435.

3. Котенко И. В., Степашкин М.В., Котенко Д.И., Дойникова Е.В. Оценивание защищенности информационных систем на основе построения деревьев социо-инженерных атак // Известия высших учебных заведений. Приборостроение. 2011. Т. 54, № 12. С. 5–9. ISSN: 0021-3454, eISSN: 2500-0381.

4. Середкин М.Д., Атомян А.С., Моргунов В.М. Классификация компьютерных атак на основе деревьев решений // Методы и технические средства обеспечения безопасности информации. 2019. № 28. С. 107–108. ISSN: 2305-994X.

5. Чечулин А.А. Построение и анализ деревьев атак на компьютерные сети с учетом требования оперативности: дис. … канд. техн. наук: 05.13.19. СПб.: С.-Петерб. ин-т информатики и автоматизации РАН, 2013. 152 с.

6. Linets G.I., Melnikov S.V. Criterion for identification of the probability model of the state of satellite communication channels // Современная наука и инновации. 2020. № 2 (30). С. 29–36.

7. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): сайт. URL: http://fstec.ru (дата обращения: 23.02.2023).

8. Сапиев А.З. Идентификация пользователей сети по клавиатурному почерку // Вестник Вологодского государственного университета. Серия: Технические науки. 2020. № 4 (10). С. 45–46.

9. Пащенко Д.В., Бальзанникова Е.А. Метод идентификации пользователя по клавиатурному почерку с использованием модели доверия // XXI век: итоги прошлого и проблемы настоящего плюс. 2021. № 3 (55). С. 96–99. DOI: 10.46548/21vek-2021-1055-0018, ISSN: 2221-951X.

10. Казачук М.А. Динамическая аутентификация пользователей на основе анализа работы с клавиатурой компьютера: дис. … канд. физ.-мат. наук: 05.13.11. М.: Моск. гос. ун-т им. М.В. Ломоносова, 2019. 155 с.

11. Исследование системы идентификации и подтверждения легитимности доступа на основе динамических методов биометрической аутентификации / М.М. Путято, А.С. Макарян, Ш.М. Чич, В.К. Маркова // Прикаспийский журнал: управление и высокие технологии. 2020. № 3 (51). С. 83–93. DOI: 10.21672/2074-1707.2020.51.1.083-093, ISSN: 2074-1707.

12. Артюшина Л.А., Троицкая Е.А. Некоторые подходы к оценке информативности параметров идентификации пользователя по клавиатурному почерку на основе поведенческой биометрии // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2022. Т. 22, № 3. С. 30–38. DOI: 10.14529/ctcr220303

13. Разработка вероятностной-имитационной математической модели формирования параметров поврежденности обработанной поверхности при двукратном технологическом воздействии / А.И. Денчик, Ж.К. Мусина, А.Ж. Касенов, Л.Р. Мусина // Наука и техника Казахстана. 2022. № 1. С. 28–39. DOI: 10.48081/JGZE9345

14. Дородников Н.А. Разработка методики повышения уровня защищённости вычислительных сетей на основе вероятностной поведенческой модели, использующей деревья атак: дис. … канд. техн. наук: 05.13.19. СПб.: С.-Петерб. нац. исслед. ун-т информац. технологий, механики и оптики, 2017. 185 с.

15. Кожомбердиева Г.И., Бураков Д.П., Хамчичев Г.А. Разработка программ для поддержки принятия решений на основе байесовских вероятностных моделей // Программные продукты и системы. 2022. № 2. С.184–194. DOI: 10.15827/0236-235X.138.184-194

References

1. Alpeyev E.V., Stadnik A.N., Skryl S.V. A method of predicting computer attacks based on determining the weights of attributes of a computer attack using the decision tree method. Electronic network polythematic journal "Scientific Works of the Kuban State Technological University". 2021;6:82–92. (In Russ.) ISSN: 2306-1456.

2. Klyaus T.K., Gatchin Yu.A. Probability evaluation of attacks on information system using event tree analysis. Journal of the Ural Federal district. Information security. 2018;4(30):31–37. (In Russ.) DOI: 10.14529/secur180405, ISSN: 2225-5435.

3. Kotenko I.V., Stepashkin M.V., Kotenko D.I., Doynikova E.V. Assessment of information system protectability on the base of development of tree of social engineering attack. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie = Journal of Instrument engineering*. 2011;54(12):5–9. (In Russ.) ISSN: 0021-3454, eISSN: 2500-0381.

4. Seredkin M.D., Atomyan A.S., Morgunov V.M. [Classification of computer attacks based on decision trees]. *Metody i tekhnicheskiye sredstva obespecheniya bezopasnosti informatsii*. 2019;28:107–108. (In Russ.) ISSN: 2305-994X.

5. Chechulin A.A. *Postroyeniye i analiz derev'yev atak na komp'yuternyye seti s uchetom trebovaniya operativnosti: dis. kand. tekhn. nauk: 05.13.19* [Construction and analysis of attack trees on computer networks, taking into account the requirements of efficiency. Cand. sci. diss.]. St. Petersburg: St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences; 2013. 152 p. (In Russ.)

6. Linets G.I., Melnikov S.V. Sriterion for identification of the probability model of the state of satellite communication channels. *Modern Science and Innovations*. 2020;2(30):29–36.

7. *Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSEK Rossii): sayt* [Federal Service for Technical and Export Control (FSTEC of Russia): website]. (In Russ.) Available at: http://fstec.ru (accessed 23.02.2023).

8. Sapiev A.Z. Identification of network users by keyboard rhythm. *Bulletin of Vologda State University. Series Technical Sciences*. 2020;4(10):45–46. (In Russ.)

9. Pashchenko D.V., Balzannikova E.A. A method for identifying a user by keyboard handwriting using a trust model. *XXI Century: Resumes of the Past and Challenges of the Present plus*, 2021;3(55):96–99. (In Russ.) DOI: 10.46548/21vek-2021-1055-0018, ISSN: 2221-951X.

10. Kazachuk M.A. *Dinamicheskaya autentifikatsiya pol'zovateley na osnove analiza raboty s klaviaturoy komp'yutera: dis. kand. fiz.-mat. nauk: 05.13.11* [Dynamic user authentication based on computer keyboard operation analysis. Cand. sci. diss.]. Moscow: Lomonosov Moscow State University; 2019. 155 p. (In Russ.)

11. Putyato M.M., Makaryan A.S., Chich Sh.M., Markova V.K. System development for identification and confirmation of access legitimacy based on biometric authentication dynamic methods. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii = Caspian journal: control and high technologies*. 2020;3(51):83–93. (In Russ.) DOI: 10.21672/2074-1707.2020.51.1.083-093, ISSN: 2074-1707.

12. Artyushina L.A., Troitskaya E.A. Some approaches to assessing the informative of user identification parameters by keyboard handwriting based on behavioral biometrics. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2022;22(3):30–38. (In Russ.) DOI: 10.14529/ctcr220303

13. Denchik A.I., Musina Zh.K., Kasenov A.Zh., Musina L.R. Development of a probabilistic simulation mathematical model for the formation of damage parameters of a treated surface under a two-time technological impact. *Science and Technology of Kazakhstan*. 2022;1:28–39. (In Russ.) DOI: 10.48081/JGZE9345

14. Dorodnikov N.A. *Razrabotka metodiki povysheniya urovnya zashchishchënnosti vychislitel'nykh setey na osnove veroyatnostnoy povedencheskoy modeli, ispol'zuyushchey derev'ya atak: dis. kand. tekhn. nauk: 05.13.19* [Development of a technique for increasing the level of security of computer networks based on a probabilistic behavioral model using attack trees. Cand. sci. diss.]. St. Peters-

burg: St. Petersburg National Research University of Information Technologies, Mechanics and Optics; 2017. 185 p. (In Russ.)

15. Kozhomberdieva G.I., Burakov D.P., Khamchichev G.A. Development of decision support programs based on Bayesian probabilistic models. *Software & Systems*. 2022;2:184–194. (In Russ.) DOI: 10.15827/0236-235X.138.184-194

Информация об авторе

Артюшина Лариса Андреевна, канд. пед. наук, магистр направления «Информационные системы и технологии», доц. кафедры информатики и защиты информации, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; larisa-artusina@yandex.ru.

Information about the author

Larisa A. Artyushina, Cand. Sci. (Education), Master's degree in Information Systems and Technologies, Ass. Prof. of the Department of Informatics and Information Protection, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; larisa-artusina@yandex.ru.

Статья поступила в редакцию 24.02.2023

The article was submitted 24.02.2023