УДК 004.056 + 003.26 Вестник УрФО № 4(30) / 2018, с. 31–37

Кляус Т. К., Гатчин Ю. А.

DOI: 10.14529/secur180405

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ С ПОМОЩЬЮ ДЕРЕВЬЕВ СОБЫТИЙ

В статье рассматриваются графические подходы к анализу возможных сценариев реализации угроз в информационных системах, основанные на использовании направленных ациклических графов. Рассматриваются особенности применения деревьев атак в качестве инструмента оценки безопасности информационной системы. Предлагается подход для определения вероятностей реализации атак на информационную систему на основе метода анализа деревьев событий. Для иллюстрации предлагаемого подхода на основе данных каталога общих шаблонов атак CAPEC построена блок-схема алгоритма прогнозирования вероятностей реализации атак на идентификаторы сеанса и ресурсов.

Ключевые слова: *информационная безопасность, атака, деревья атак, деревья событий, оценка рисков безопасности*

Klyaus T. K., Gatchin Yu. A.

PROBABILITY EVALUATION OF ATTACKS ON INFORMATION SYSTEM USING EVENT TREE ANALYSIS

The article deals with graphical approaches to analysis of possible information systems threats realization scenarios based on the use of directed acyclic graphs. The features of attack trees usage as a tool for information systems security assessment are considered. An approach for determining the likelihood of attacks realization based on the event tree analysis is proposed. To illustrate the proposed approach, a block scheme for predicting the likelihood of attacks on session and resource IDs based on the catalog of common attack patterns (CAPEC) is built.

Keywords: *information security, attack, attack trees, event trees, information security risk assessment.*

Вследствие постоянного усложнения архитектуры информационных систем (ИС), роста числа уязвимостей в используемом программном обеспечении (ПО), улучшения технических возможностей потенциальных нарушителей, на предприятиях и в организациях возникает необходимость в разработке модели угроз (атак), необходимой для после-

дующего определения перечня мер и средств защиты информации. Как правило, проблема выбора средств защиты информации (СЗИ) представляет собой оптимизационную задачу выбора при заданных ограничениях минимизации стоимости при требуемой эффективности мер защиты или максимизации эффективности мер защиты при ограничении на стоимость средств [1].

При разработке модели угроз наибольший интерес для специалистов по информационной безопасности представляют угрозы, обусловленные действиями субъекта (антропогенные угрозы), поскольку вероятности возникновения угроз, источниками которых являются технические средства, могут быть рассчитаны с помощью методов теории надежности, а вероятности стихийных бедствий и природных катастроф могут быть определены на основе статистических данных или рассчитаны на этапах проектирования, строительства и эксплуатации объектов (помещений). В настоящее время широкое распространение получили графические подходы к представлению и анализу сценариев реализации угроз, основанные на использовании направленных ациклических графов. Графические подходы обладают рядом преимуществ: они наглядны, позволяют представить атаки (угрозы, уязвимости) в иерархическом виде, позволяют производить качественный и количественный анализ, для некоторых подходов существует программное обеспечение для проведения расчетов. Наиболее подробное описание графических подходов, основанных на использовании направленных ациклических графов, приведено в исследовании [2]. Авторы данной статьи группируют рассматриваемые ими формализмы, опираясь на два основных критерия:

— Моделирует ли рассматриваемый подход атаки и (или) защитные меры;

— Является ли подход статическим (временной аспект не учитывается) или последовательностным (временной аспект влияет на рассматриваемые действия).

Классификация подходов к моделированию атак, предложенная в статье [2], представлена на рис. 1.

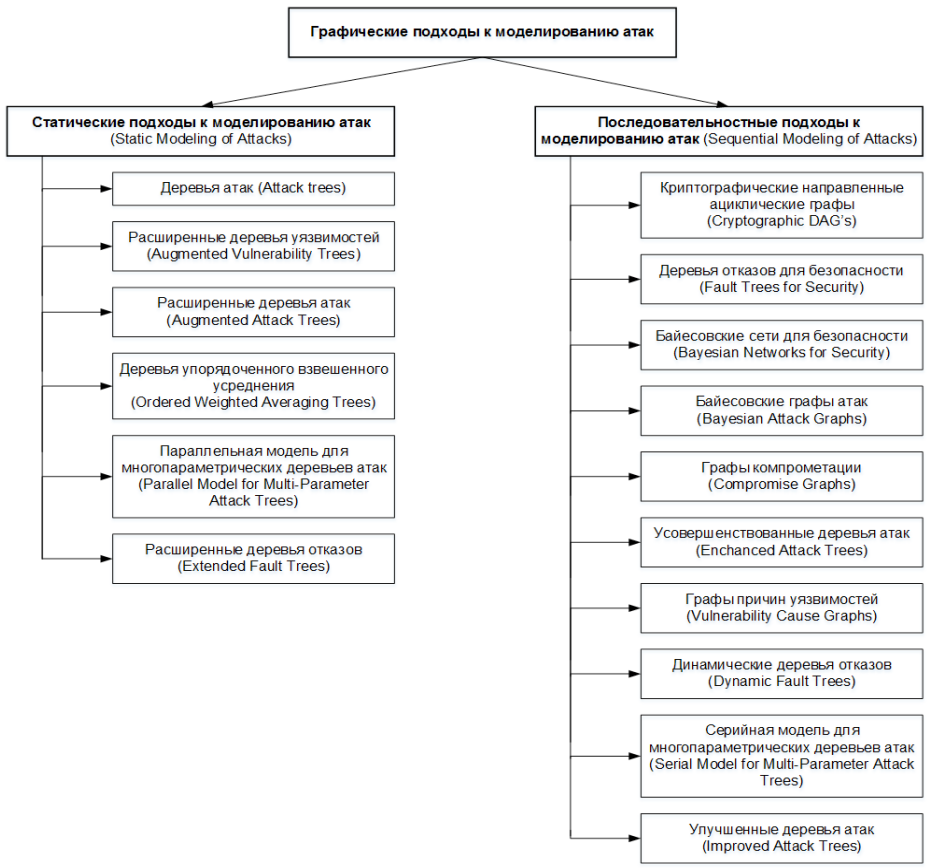

Рис. 1. Классификация графических подходов к моделированию атак [2]

Наиболее популярным подходом к анализу возможных способов реализации угроз и представления их в структурированном

виде являются деревья атак. Понятие деревьев атак было популяризировано Б. Шнайером [3] в качестве инструмента для оценки безопасности систем. Прототипом деревьев атак являются деревья отказов, применяющиеся в теории надежности и служащие для графического описания комбинаций событий, приводящих к отказу системы [4].

Дерево атак представляет собой связный граф, не содержащий циклов и кратных ребер. Вершина дерева (корневой узел) обозначает конечную цель атакующей стороны. Вершины, соединенные ребрами с корнем дерева, представляют собой действия атакующей стороны, которые она предпринимает для достижения поставленной цели. Конечная вершина, из которой не выходит ни одного нового ребра, называется листовым узлом и представляет собой действие атакующей стороны или защитную меру, которая не может быть разложена на составляющие. Вершины, не являющиеся листовыми узлами или корнем, называются узлами ветвления. Узлы ветвления представляют собой промежуточные состояния или подцели атакующего и обозначаются как узлы «И» (конъюнктивные узлы) или узлы «ИЛИ» (дизъюнктивные узлы). Для того, чтобы была достигнута цель узла «И», все исходящие из него вершины должны быть истинными – должно выполняться каждое действие злоумышленника из всей совокупности дочерних элементов узла ветвления. Истинное состояние узла «ИЛИ» достигается в случае, если хотя бы один из его дочерних элементов принимает истинное значение.

В настоящее время исследования деревьев атак фокусируются на улучшении эффективности формализма [5], а также на основе совместного использования деревьев атак с другими формализмами – сетями Байеса [6], сетями Петри [7], деревьями отказов [8] и методом вариантов злоупотребления (misuse cases) [9].

Широкое применение деревьев атак объясняется возможностью их использования как для качественного, так и для количественного анализа рисков. С помощью метода восходящего анализа (присвоения значений атрибутов листовым узлам и дальнейшего расчета значения для корневого узла) могут быть найдены такие атрибуты, как: затраты на проведение атаки, ее трудность и вероятность успешного проведения, наличие специальных навыков и оборудования у атакующей стороны и т.д. Области значений атрибутов могут варьироваться в зависимости от их содержания: это могут быть булевы значения, значения номинальной шкалы, действительные числа, а также дискретные или непрерывные распределения вероятностей [10]. Одним из наиболее часто рассчитываемых с помощью деревьев атак атрибутов является вероятность успешной реализации атаки [8, 11], поскольку определение ее значения необходимо для оценки рисков информационной безопасности.

В данной работе предлагается противоположный подход для расчета значений вероятностей атак на ИС, а именно, выполнение анализа дерева атак с корневого узла, поскольку данный подход также базируется на хорошо проработанной методической основе. За основу взят метод анализа деревьев событий (ETA – Event Tree Analysis), рекомендованный ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» [12] и представляющий собой графический метод представления взаимоисключающих последовательностей событий, следующих за появлением исходного события. Данный метод применяется как для качественной, так и для количественной оценки рисков. Количественная оценка рисков, в отличии от качественной, предполагает использование точных численных значений для ряда параметров, необходимых для расчета рисков безопасности (вероятности или прогнозируемого числа инцидентов, следствием которых может быть нанесение ущерба активам организации, величины ущерба, частоты возникновения угроз и т.д.). Качественная оценка рисков основывается на описании сценариев угроз, для анализа которых применяется фиксированная шкала значений (например, «низкий», «средний», «высокий»).

Каждая ветвь дерева событий представляет собой вероятность того, что все события на этом пути произойдут, поэтому вероятность результата вычисляют как произведение отдельных условных вероятностей и вероятности начального события при условии независимости событий.

К основному преимуществу метода ETA относят возможность анализа сценариев развития событий после возникновения начального события. Недостатком является то, что реализация каждого последующего события обусловлена сочетанием событий, произошедших в предыдущих точках ветвления схемы дерева событий, что вызывает необходи-

мость рассматривать все взаимосвязи по возможным путям развития событий [12].

Для реализации в данной статье метода ETA представим дерево атак на ПО (рис. 2), корневым узлом которого является нарушение конфиденциальности информации, контроля доступа и авторизации путем реализации атак на идентификаторы сеанса и ресурсов. Данный пример дерева атаки был построен на основе данных каталога общих шаблонов атак CAPEC (Common Attack Pattern Enumeration and Classification), созданного Министерством внутренней безопасности США в рамках стратегической инициативы Software Assurance (SwA) Управления кибербезопасности и коммуникаций (CS&C) [13]. Каталог шаблонов атак CAPEC и список недостатков программного обеспечения CWE (Common Weakness Enumeration) поддерживаются MITRE Corporation [14].

Вероятность атаки с использованием доверенных учетных данных примем равной 1,0. Условные вероятности в узлах ветвления определяют вероятность наступления указанного события на основе критерия «да» или «нет», при этом сумма вероятностей, определяющих оба события, принимается равной 1,0. Условная вероятность листовых событий определяется произведением вероятностей, определенных в предшествующих узлах ветвления. Полученные значения дают оценку расчетного прогноза условных вероятностей атак с использованием доверенных учетных данных, которые может предпринять атакующая сторона. Сумма условных вероятностей, соответствующих атакам, указанным в листовых узлах, также равна 1,0.

Значения вероятностей событий для прогнозирования вероятностей атак присваиваются на основании имеющихся данных о не-

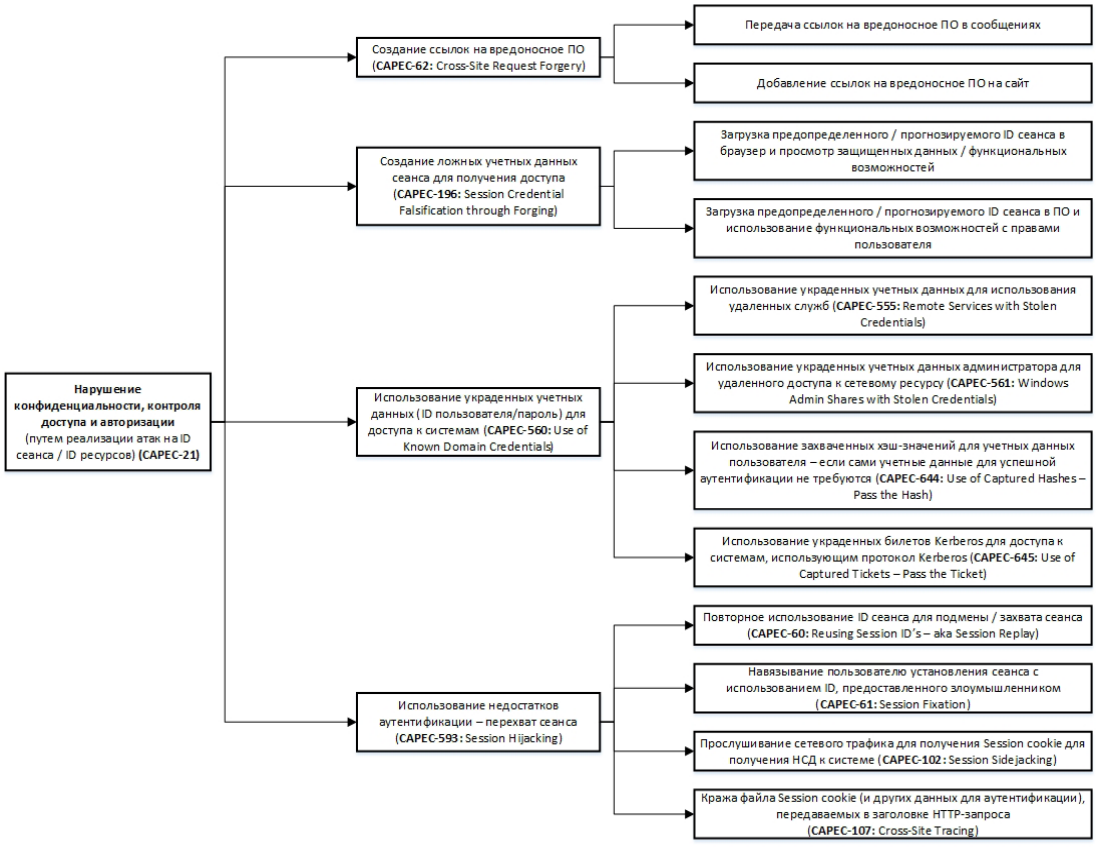

Рис. 2. Дерево атак на идентификаторы сеанса и ресурсов, построенное на основе каталога общих шаблонов атак CAPEC

Представим построенное дерево виде блок-схемы, в которой корневой узел располагается в левом верхнем углу. Узлы ветвления и листовые узлы изображаются в виде ромбов и прямоугольников, соответственно (рис. 3).

достатках и уязвимостях, которыми обладает рассматриваемое ПО и которыми может воспользоваться атакующая сторона. Данная оценка вероятности зависит от точности экспертных оценок вероятностей наступления

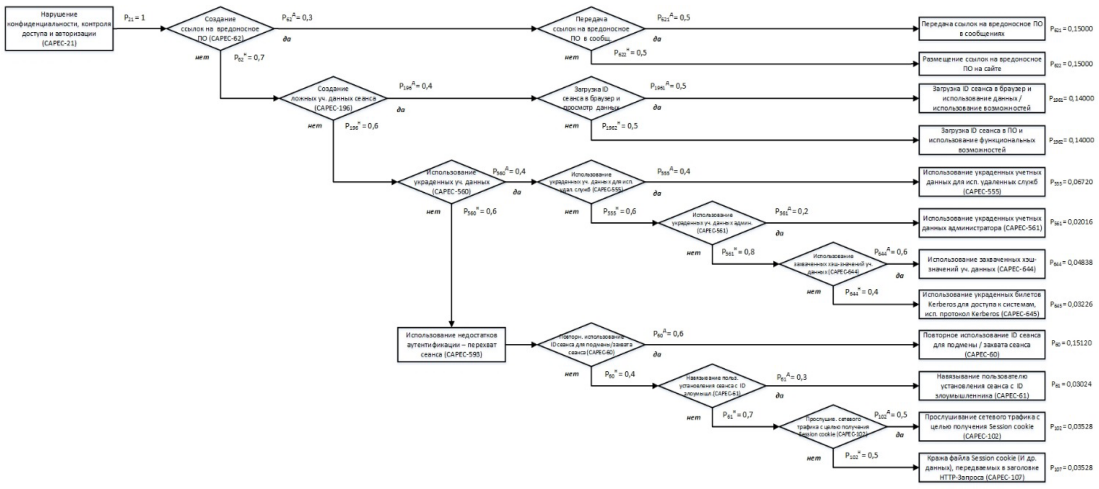

Рис. 3. Блок-схема алгоритма прогнозирования вероятности атак на идентификаторы сеанса и ресурсов с целью нарушения конфиденциальности информации, контроля доступа и авторизации с присвоенными и рассчитанными значениями вероятностей атак

событий в узлах ветвления. Для иллюстрации предлагаемого в настоящей работе подхода на рис. 3 приведен пример расчета вероятностей атак, основанных на использовании доверенных учетных данных. Для присвоения значений вероятностей атак был проанализирован ряд параметров, указанных в каталоге общих шаблонов атак CAPEC: вероятность реализации атаки, степень серьезности последствий реализации атаки, уровень требуемых навыков злоумышленника и количество соответствующих недостатков программного обеспечения CWE.

В настоящее время наблюдается широкое применение графических подходов к моделированию атак и защитных мер – они используются для анализа состояния информационной безопасности в системах SCADA, системах голосования, мобильной связи, для анализа удаленных и социотехнических атак [2]. Наиболее распространенным графическим подходом к моделированию атак являются деревья атак, представляющие собой модель, с помощью которой легко представляются схемы последовательных действий, при этом используется классический алгоритмический аппарат [15]. Существует тенденция интеграции деревьев атак с другими формализмами. В настоящей работе предлагается подход к определению вероятности реализации атак на основе метода анализа деревьев событий – в данном случае для расчета вероятностей используется нисходящий, а не восходящий подход, применяемый при анализе деревьев атак. Данный подход позволяет выполнять количественный и качественный анализ возможных атак на ИС, в дальнейшем полученные с его помощью результаты могут использоваться в расчетах при оценке рисков безопасности ИС. Однако необходимо отметить, что для выполнения корректного количественного анализа деревьев событий существует проблема поиска статистических данных об атаках.

Литература

1. Хализев В.Н., Кузьмин Д.И. Методика выбора оптимального набора средств программно-аппаратной защиты информации // Физико-математические науки и информационные технологии: проблемы и тенденции развития: сб. ст. по матер. VIII междунар. науч.-практ. конф. – 2012. – № 8. – С. 102-107.

2. Kordy B., Pietre-Cambacedes L., Schweitzer P. DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees // Computer Science Review. – 2014. – Vol. 13-14. – P. 1-38.

3. Schneier B. Attack trees // Dr. Dobb's Journal of software tools. – 1999. – № 24(12). – P. 21-29.

4. Кляус Т.К., Гатчин Ю.А. Применение графического представления атак в моделировании угроз безопасности информации // Научно-технический вестник Поволжья. – 2017. – № 3. – С. 108-110.

5. Gadyatskaya O., Trujillo-Rasua R. New Directions in Attack Tree Research: Catching up with Industrial Needs // GraMSec 2017: 4th International Workshop on Graphical Models for Security. – 2017. – P. 115-126.

6. Gribaudo M., Iacono M., Marrone S. Exploiting Bayesian Networks for the Analysis of Combined Attack Trees // Electronic Notes in Theoretical Computer Science. – 2015. – Vol. 310. – P. 91-111.

7. Dalton G.C., Mills R.F., Colombi J.M., Raines R.A. Analyzing Attack Trees using Generalized Stochastic Petri Nets // Proceedings of the 2006 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY. – 2006. – P. 116-123.

8. Fovino I.N., Masera M., De Cian A. Integrating cyber attacks within fault trees // Reliability Engineering & System Safety. – 2009. – Vol. 94(9). – P. 1394–1402.

9. Tondel I. A., Jensen J., Rostad L. Combining Misuse Cases with Attack Trees and Security Activity Models // 2010 International Conference on Availability, Reliability and Security. – 2010. – P. 438-445.

10. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees // International journal of secure software engineering. – 2012. – Vol. 3(2). – P. 1-35.

11. Edge K.S., Dalton D.C., Raines R.A., Mills R.F. Using attack and protection trees to analyze threats and defenses to homeland security // MILCOM'06 Proceedings of the 2006 IEEE conference on Military communications. – 2006. – P. 953-959.

12. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска // Москва: Стандартинформ. – 2012.

13. CAPEC – Common Attack Pattern Enumeration and Classification // A community resource for identifying and understanding attacks. URL: https://capec.mitre.org/ (дата обращения: 03.10.2018)

14. MITRE // The MITRE Corporation. URL: https://www.mitre.org/ (дата обращения: 03.10.2018)

15. Кляус Т. К., Наумов А. Д., Гатчин Ю. А., Бондаренко И. Б. Сравнительное исследование применимости деревьев атак-контрмер и метода куста событий для оценки безопасности информационных систем // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 2(28). – С. 36-42.

References

1. Halizev V.N., Kuz'min D.I. Metodika vybora optimal'nogo nabora sredstv programmno-apparatnoj zashchity informacii. Fiziko-matematicheskie nauki i informacionnye tekhnologii: problemy i tendencii razvitiya: sb. st. po mater. VIII mezhdunar. nauch.-prakt. konf., 2012, no. 8, pp. 102-107.

2. Kordy B., Pietre-Cambacedes L., Schweitzer P. DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees. Computer Science Review, 2014, Vol. 13-14, pp. 1-38.

3. Schneier B. Attack trees. Dr. Dobb's Journal of software tools, 1999, no. 24(12), pp. 21-29.

4. Klyaus T.K., Gatchin Ju.A. The Use of Attacks Graphical Representation for Threat Modeling [Primenenie graficheskogo predstavlenija atak v modelirovanii ugroz bezopasnosti informacii]. Nauchno-tehnicheskij vestnik povolzh'ja [Scientific and Technical Bulletin of the Volga Region], 2017, no. 3, pp. 108-110.

5. Gadyatskaya O., Trujillo-Rasua R. New Directions in Attack Tree Research: Catching up with Industrial Needs. GraMSec 2017: 4th International Workshop on Graphical Models for Security, 2017, pp. 115-126.

6. Gribaudo M., Iacono M., Marrone S. Exploiting Bayesian Networks for the Analysis of Combined Attack Trees. Electronic Notes in Theoretical Computer Science, 2015, Vol. 310, pp. 91-111.

7. Dalton G.C., Mills R.F., Colombi J.M., Raines R.A. Analyzing Attack Trees using Generalized Stochastic Petri Nets. Proceedings of the 2006 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, 2006, pp. 116-123.

8. Fovino I.N., Masera M., De Cian A. Integrating cyber attacks within fault trees. Reliability Engineering & System Safety, 2009, Vol. 94(9), pp. 1394–1402.

9. Tondel I. A., Jensen J., Rostad L. Combining Misuse Cases with Attack Trees and Security Activity Models. 2010 International Conference on Availability, Reliability and Security, 2010, pp. 438-445.

10. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees. International journal of secure software engineering, 2012, Vol. 3(2), pp. 1-35.

11. Edge K.S., Dalton D.C., Raines R.A., Mills R.F. Using attack and protection trees to analyze threats and defenses to homeland security. MILCOM'06 Proceedings of the 2006 IEEE conference on Military communications, 2006, pp. 953-959.

12. GOST R ISO/IEC 31010-2011. Risk management. Risk assessment techniques. Moscow, Standartinform, 2012.

13. CAPEC – Common Attack Pattern Enumeration and Classification. A community resource for identifying and understanding attacks. Available at: https://capec.mitre.org/

14. The MITRE Corporation. Available at: https://www.mitre.org/

15. Klyaus T. K., Naumov A. D., Gatchin Yu. A., Bondarenko I. B. A Comparative Study of Attack-Defense Trees and Event Bush Method Applicability for Information Systems Security Assessment [Sravnitel'noe issledovanie primenimosti derev'ev atak-kontrmer i metoda kusta sobytij dlya ocenki bezopasnosti

informacionnyh sistem]. Vestnik UrFO. bezopasnost' v informacionnoj sfere [UrFR Newsletter. Information Security], 2018, no. 2(28), pp. 36-42.

КЛЯУС Татьяна Константиновна, аспирант кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: t_klyaus@corp.ifmo.ru

ГАТЧИН Юрий Арменакович, доктор технических наук, профессор кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: gatchin@mail.ifmo.ru

KLYAUS Tatiana, postgraduate student of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: t_klyaus@corp.ifmo.ru

GATCHIN Yurii, doctor of technical sciences, professor of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: E-mail: gatchin@mail.ifmo.ru