УДК 004.942 + 519.157 Вестник УрФО № 4(46) / 2022, с. 52–57

Бердюгин В.Ю., Аверьянов А.А., Шадрив В.В.

DOI: 10.14529/secur220406

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ УГРОЗ ФИЗИЧЕСКОГО ПРОНИКНОВЕНИЯ ЗЛОУМЫШЛЕННИКА НА ЗАЩИЩЕННЫЙ ОБЪЕКТ

Для современных объектов информатизации одной из наиболее актуальных проблем является повышение эффективности или создание эффективной защиты от угроз, связанных с неправомерным физическим доступом к защищаемым информационным объектам. При этом возникает потребность в объективной оценке как вероятности реализации подобных угроз, так и эффективности организационных и инженерно-технических средств их реализации. В работе представлен результат разработки математической модели, на основе которой возможно решение перечисленных задач.

Ключевые слова: *математическое моделирование, информационная безопасность, дискретная математика, система безопасности, инженерно-техническая защита информации, оценка защищенности, объект информатизации.*

Berdugin V.U., Averyanov A.A., Shadriv V.V.

MATHEMATICAL MODEL FOR ASSESSING THREATS OF PHYSICAL INTRUSION OF AN INTRUDER INTO A PROTECTED OBJECT

For modern informatization objects, one of the most pressing problems is to increase the efficiency or create effective protection against threats associated with unlawful physical access to protected information objects. At the same time, there is a need for an objective assessment of both the likelihood of such threats and the effectiveness of organizational and engi-

neering means of their implementation. The paper presents the result of the development of a mathematical model, on the basis of which it is possible to solve the listed problems.

Keywords: *mathematical modeling, information security, discrete mathematics, security system, engineering and technical protection, security assessment, information object.*

Ввиду разнообразия и уникальности каждого объекта, на котором обрабатывается защищаемая информация, разработка системы физической защиты является трудоемким процессом, в котором для каждого объекта требуется индивидуальный подход. Создание системы защиты требует значительного количества ресурсов, но не всегда эти ресурсы расходуются эффективно [1]. Под «защищаемым» объектом будем понимать объект, обладающий определенной степенью защищенности и нуждающийся в модернизации защиты, а также оптимизации ресурсов, затрачиваемых на защиту.

Согласно пункту 2.4 Методики оценки угроз безопасности информации, утвержденной ФСТЭК России 5 февраля 2021 года [2] (далее – Методика) оценка угроз безопасности информации должна носить систематический характер и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии и модернизации систем. По результатам такой оценки должны быть выявлены актуальные угрозы, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах информации и (или) к нарушению, прекращению функционирования этих систем. Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем [2].

Оценка угроз проводится на всех этапах разработки систем защиты объектов. На этапе создания систем результаты оценки угроз безопасности информации должны быть направлены на обоснование выбора организационных и технических мер по защите информации (обеспечению безопасности), а также на выбор средств защиты информации и их функциональных возможностей [2]. При этом на этапе эксплуатации систем защиты в результате оценки могут быть найдены дополнительные угрозы безопасности. В этом случае по ним должны быть предложены обоснованные меры по улучшению или созданию систем защиты. Обобщая вышесказанное, можно сделать вывод о том, что для обеспечения высокого уровня безопасности информации нужно постоянно и в полном объеме проводить мероприятия по оценке и улучшению систем безопасности.

В связи с необходимостью постоянного проведения оценки безопасности на разных объектах, особый интерес представляют программные решения, эффективно моделирующие и рассчитывающие возможные пути проникновения, а также способы их устранения и решения, уменьшающие или полностью исключающие влияние человеческого фактора на расчёт защищенности объекта. Нормативные акты так же не противоречат использованию данных решений: пункт 2.9 Методики разрешает при оценке угроз безопасности использовать программные средства, позволяющие автоматизировать данную деятельность.

Исследование и моделирование систем физической защиты широко представлено в работах как отечественных, так и зарубежных ученых. Так, М.Гарсия в своей работе по проектированию и оценке систем физической защиты рассмотрел подходы к проектированию, анализу и оценке систем физической защиты [3], уделил большое внимание разным типам внешних и внутренних датчиков, средств связи, приборам, применяемым для обнаружения оружия, наркотических и взрывчатых веществ, и др. А.С. Боровский в своей работе [4] представил собственный метод обоснования требований (показателей качества) к системам физической защиты, разработал модифицированный алгоритм Дейкстры для поиска наименее защищенного пути с использованием нечетких чисел и т.д. И.М. Янников представил структурную схему интеллектуальной интегрированной системы безопасности критически важных и потенциально опасных объектов [5]. А.Д. Тарасов в 2017 году спроектировал систему физической защиты с использованием адаптивного генетического алгоритма [6], который содержит в себе алгоритм для расчета безопасности территории объекта. В 2019 году А.Д. Япаров предложил алгоритм имитационного мо-

делирования угрозы физического доступа к значимому объекту критической информационной инфраструктуры [7].

Однако, по нашему мнению, перечисленные выше модели и прилагающиеся к ним программные решения либо применимы только на стадии тестирования систем физической защиты, либо не обладают достаточной гибкостью. Ситуация усугубляется отсутствием нормативной базы для определения и стандартизации систем физической защиты информации [8].

Задачей представленной работы является создание модели, учитывающей варианты проникновения злоумышленника на защищаемые объекты с целью повышения эффективности систем защиты.

Предлагаемая модель учитывает все возможные пути проникновения со стороны злоумышленника, так как в реальности невозможно оценить какой информацией, навыками и знаниями обладает злоумышленник, проникающий на объект (далее – нарушитель), а также учесть все средства получения доступа к информации о защищенном объекте. Для построения общей модели нарушителя определены следующие условия:

• нарушителю известна подробная информацию об объекте, план здания со всеми средствами защиты;

• нарушитель использует все возможные технические средства проникновения на объект;

• нарушитель стремится оптимизировать свой путь проникновения на объект.

При этом модель защищаемого объекта представлена в виде расширенного мультиграфа, что позволяет учитывать дополнительную информацию, в частности, замки для ребер, ключи и ценность информации для вершин. Вершиной такого графа являются определенные позиции внутри защищаемого объекта. Ребро же – путь перехода нарушителя от одной вершины в другую. Например, в случае, если принять вершину за комнату, то ребрами будут являться коридоры, по которым можно перейти в эту комнату. На рис. 1 представлен пример используемого графа.

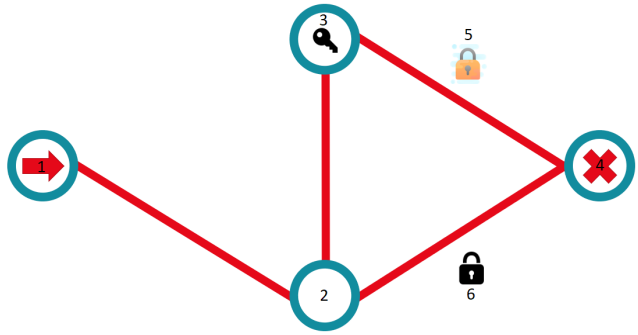

Рис. 1. Пример графа с моделью «ключи-замки»

Разработанная модель подразумевает использование устройств физической защиты, требующих наличия «ключа» для последующего доступа. При этом подразумевается, что замки устанавливаются как средство защиты от физического проникновения и к каждому ключу есть замок (но не к каждому замку есть ключ). На рис. 1 расположены два замка: 5 и 6 на переходах из вершин 3 и 2 в 4 соответственно. Ключ, расположенный в вершине 3 подходит только для замка 6. Если у нарушителя нет ключа от замка, он должен приложить некоторые усилия для преодоления данного замка. Под замком может подразумеваться не только устройство, закрывающее двери: как замок можно рассматривать, например, охранника – он будет замком без ключа (как, например, замок 5 на рис. 1). Нарушителю необходимо будет приложить определенные усилия для преодоления замка. На рис. 1 точка проникновения нарушителя на объект обозначена цифрой 1, целевая точка – цифрой 4. После попадания нарушителя в вершину 1 у него есть только один путь, после перехода по нему в вершину 2 у него появляется выбор: он может взломать замок 6 (т.е. затратить определенное количество усилий), или же перейти в вершину 3, взять ключ и, вернувшись в 2, открыть замок 6 и проникнуть в целевую вершину 4. Нарушитель так же может перейти в вершину 3 и попытаться взломать замок 5 и пройти в вершину 4. В конечном итоге мы имеем полный набор возможных путей проникновения нарушителя и понимание того, какой из путей требуется защитить. Таким образом, можно

представить и распределить практически любые меры защиты и создать систему физической защиты высокого уровня.

Сформулируем задачу математически. Пусть некоторый объект имеет некоторое множество путейпроникновения к конечной точке (защищаемой информации, например: серверу). Если к конечной точке нет путей проникновения, то задача является бессмысленной, поскольку нарушитель не может проникнуть к защищаемой информации каким-либо способом, то есть, считаем, что множество не пусто.

Далее определим некоторое подконтрольное множество ребер, которое не является пустым, поскольку если на текущую ситуацию повлиять невозможно, то задача является бессмысленной.

Для учета имеющихся у заказчика ресурсов для физической защиты информации – финансов и технического обеспечения, которые могут быть использованы или используются при защите, введена величина «капитал защиты» X. Пусть S – это множество распределений X. Таким образом, имеется множество вариантов распределения X на конечное множествор E. При этом, если есть хотя бы одно подконтрольное ребро, то имеется хотя бы один вариант распределения капитала защиты: S ≠ ∅.

Также, для каждого пути p из множества всех путей p ∈ P определим множество подконтрольных ребер, которые в него входят $E' \subseteq E$. Оно не может являться пустым, поскольку если нарушитель имеет способ получения информации, не подконтрольный нам, то задача является бессмысленной. В итоге получим выражение:

$$e(p) = E', \quad (1)$$

где $p \in P$; $E' \subseteq E$; $E' \neq \emptyset$.

Далее определим сложность преодоления нарушителем конкретного пути ω' при текущем распределении капитала защиты s ∈ S для каждого пути p ∈ P:

$$\omega(p,s) = \omega', \quad (2)$$

где $\omega' \in \mathbb{R}+$; $p \in P$; $s \in S$.

В итоге требуется выбрать оптимальное распределение весов, при котором вес пути с минимальным весом $min_{p\in P}\omega(p,s)$ будет максимален $max_{s\in S}$:

$$r(P,S) = max_{\ s\in S}(min_{\ p\in P}\,\omega\,(p,s)). \quad (3)$$

При этом функция расчета веса для пути ω является непрерывно возрастающей, а ее производная стремиться к нулю:

$$\omega(p,s) = \sum_{e\,\in\, e(p)} \frac{\sqrt[3]{\omega'(e,s)}}{\sum_{e\,\in\, E}\sqrt[3]{\omega'(e,s)}}, \quad (4)$$

где $p \in P$; $s \in S$.

В (4) представлены абсолютные значения весов $\omega' \in \mathbb{R}$ из текущего варианта распределения капитала защиты $s \in S$ на ребре $e \in P$:

$$\omega'(e,s) = \omega'_i,$$

где $\omega'_i \in \mathbb{R}+$; $e \in E$; $s \in S$.

Сумма нормированных кубических корней (4) выбрана из-за простоты вычисления и ее практической применимости: чем больше будет потрачено ресурсов на то или иное ребро, тем меньший выигрыш может быть получен в дальнейшем: такой подход моделирует ситуации из реальной жизни.

Так как функция (4) не зависит от порядка разложения аргументов (имеется ввиду, что веса будут неизменны), используем итеративный подход для определения оптимального значения весов для распределения капитала защиты. Для этого введем величину ε> 0 – точность расчета распределения капитала защиты, на каждом шаге добавим ε к текущему набору весов и выберем вариант, при котором наименьший путь будет иметь максимальное значение.

Для реализации модели «ключи-замки» определим замки (для ребер) и ключи (для вершин). Тогда поиск весов для всех путей изменится: если нарушитель нашел ключ, которого у него до этого не было, то текущая вершина становится начальной вершиной пути нарушителя, а новые пути ищутся рекурсивно и добавляются к конечному пути, пройденному ранее, обнуляя при этом множество всех посещенных вершин. Определим коэффициент сложности прохода по ребру $\omega' \in \mathbb{R}$:

$$\omega(p,s) = \sum_{e\,\in\, e(p)} \frac{\sqrt[3]{\omega'(e,s)\cdot w'(e)}}{\sum_{e\,\in\, E}\sqrt[3]{\omega'(e,s)\cdot w'\,(e)}}, \quad (5)$$

где $p \in P$; $s \in S$; $w'(e) = w'_i$, где $w'_i \in \mathbb{R}+$; $e \in E$.

При отсутствии замка этот коэффициент будет равен 1, а при наличии замка он может различаться в зависимости от текущей связки ключей у нарушителя.

Чтобы учесть несколько точек, в которых хранится защищенная информация, а также обозначить их «значимость» в рамках текущей системы, вводится нормированное значение значимости защищаемой области в вершине $w''(p) \in \mathbb{R}$, на которую умножается значение, определяемое формулой (5). Это позволяет располагать веса на ребра более рационально, в зависимости от важности информации:

$$\omega(p,s) = \sum_{e\,\in\, e(p)} \frac{\sqrt[3]{\omega'(e,s)\cdot w'(e)}}{\sum_{e\,\in\, E}\sqrt[3]{\omega'(e,s)\cdot w'(e)}} \cdot w''(p), \quad (6)$$

где $p \in P$; $s \in S$; $w''(p) = w''_i$, где $w''_i \in \mathbb{R}+$; $p \in P$.

Таким образом, получено итоговое выражение для расчета системы физической защиты объекта (6), содержащего защищаемую информацию, с учетом значений весов, нескольких точек хранения защищаемой информации, наличия ключей и замков.

Построенная математическая модель может использоваться для разработки программного обеспечения, моделирующего систему защиты для помещений различного объема, корпусов защищаемых объектов и для модернизации существующих систем защиты. В качестве входных данных программного обеспечения и модели используется план здания (объекта) с указанием мест расположения средств нейтрализации неправомерного физического доступа.

Разработанная модель может быть применена для решения проблемы безопасности при защите периметра, создании защищенной сети внутри или снаружи предприятия, для улучшения защиты существующих сетей от угроз физического доступа к информации.

Литература

1. Боровский А.С. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов / А.С. Боровский, А.Д. Тарасов // Труды ИСА РАН, научный журнал. — Том 61, выпуск №1. — 2011. — С. 3–14.

2. Методика оценки угроз безопасности информации: порядок оценки угроз безопасности информации (от 5 февраля 2021 г.) // Федеральная служба по техническому и экспортному контролю. — 2021. — С. 6 – 12.

3. Гарсия М. Проектирование и оценка систем физической защиты/ М. Гарсия. — Москва: Мир, 2003. — 392 с.

4. Боровский А. С. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки системы физической защиты объектов информатизации/А. С. Боровский. // АВТОРЕФЕРАТ диссертации на соискание ученой степенидоктора технических наук. —2015.

5. Янников И.М. Структурная схема интеллектуальной интегрированной системы безопасности критически важных и потенциально опасных объектов // Известия Самарского научного центра. — 2015. —Т.17. — №6(2). —С. 570–571.

6. Тарасов А.Д. Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации // АВТОРЕФЕРАТ диссертации на соискание ученой степени кандидата технических наук. — 2017.

7. Япаров А.Д. Имитационное моделирование и оценка угроз физического доступа к значимому объекту критической информационной инфраструктуры // XVIII Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых «Безопасность информационного пространства – 2019». Сборник трудов. — 2019. — С. 98–102.

8. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. — М.: Горячая линия — Телеком, 2016. — 417 с.

9. Ищейнов В.Я. Основные положения информационной безопасности: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — М.: Форум, Инфра-М, 2015. — 208 с.

References

1. Borovskiy A.S. Integrirovannyy podkhod k razrabotke obshchey modeli funktsionirovaniya sistem fizicheskoy zashchity ob»yektov / A.S. Borovskiy, A.D. Tarasov // Trudy ISA RAN, nauchnyy zhurnal. — Tom 61, vypusk №1. — 2011. — S. 3–14.

2. Metodika otsenki ugroz bezopasnosti informatsii: poryadok otsenki ugroz bezopasnosti informatsii (ot 5 fevralya 2021 g.) // Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. — 2021. — S. 6 – 12.

3. Garsiya M. Proyektirovaniye i otsenka sistem fizicheskoy zashchity/ M.Garsiya. — Moskva: Mir, 2003. — 392 s.

4. Borovskiy A. S. Modeli, metody i algoritmy intellektual'noy podderzhki prinyatiya resheniy v zadachakh razrabotki i otsenki sistemy fizicheskoy zashchity ob"yektov informatizatsii/A. S. Borovskiy. // AVTOREFERAT dissertatsii na soiskaniye uchenoy stepenidoktora tekhnicheskikh nauk. —2015.

5. Yannikov I.M. Strukturnaya skhema intellektual'noy integrirovannoy sistemy bezopasnosti kriticheski vazhnykh i potentsial'no opasnykh ob"yektov // Izvestiya Samarskogo nauchnogo tsentra. — 2015. —T.17. — №6(2). —S. 570–571.

6. Tarasov A.D. Metod i algoritmy proyektirovaniya sistem fizicheskoy zashchity ob"yektov informatizatsii na osnove obrabotki nechetkoy informatsii // AVTOREFERAT dissertatsii na soiskaniye uchenoy stepeni kandidata tekhnicheskikh nauk. — 2017.

7. Yaparov A.D. Imitatsionnoye modelirovaniye i otsenka ugroz fizicheskogo dostupa k znachimomu ob"yektu kriticheskoy informatsionnoy infrastruktury // KHVIII Vserossiyskaya nauchno-prakticheskaya konferentsiya studentov, aspirantov i molodykh uchenykh «Bezopasnost' informatsionnogo prostranstva – 2019». Sbornik trudov. — 2019. — S. 98–102.

8. Buzov G.A. Zashchita informatsii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam / G.A. Buzov. — M.: Goryachaya liniya — Telekom, 2016. — 417 c.

9. Ishcheynov V.YA. Osnovnyye polozheniya informatsionnoy bezopasnosti: uchebnoye posobiye / V. YA. Ishcheynov, M.V. Metsatunyan. — M.: Forum, Infra-M, 2015. — 208 c.

АВЕРЬЯНОВ Антон Александрович, студент кафедры защиты информации, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: averianovaa@susu.ru

ШАДРИВ Владимир Владимирович, студент кафедры защиты информации, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: shadrivvv@susu.ru

БЕРДЮГИН Владимир Юрьевич, доцент кафедры защиты информации, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: berdiuginvi@susu.ru

AVERYANOV Anton Aleksandrovich, student of the Department of Information Security, South Ural State University. 454080, Chelyabinsk, Lenin Ave., 76. E-mail: averianovaa@susu.ru

SHADROV Vladimir Vladimirovich, Student of the Department of Information Security, South Ural State University, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: shadrivvv@susu.ru

BERDYUGIN Vladimir Yuryevich, Associate Professorof the Department of Information Security, South Ural State University, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: berdiuginvi@susu.ru