i-methods

том 13. № 1. 2021
http://intech-spb.com/i-methods/

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Математическое обеспечение оптимизации системы защиты информации в автоматизированных системах управления

Пасечник Родион Маратович
старший научный сотрудник Краснодарского высшего военного училища,
г. Краснодар, Россия, rmpasechnik@mail.ru

Табункова Марина Павловна
к.э.н., старший научный сотрудник Краснодарского высшего военного училища,
г. Краснодар, Россия, skygel@mail.ru

Королёв Игорь Дмитриевич
д.т.н., профессор кафедры Краснодарского высшего военного училища,
г. Краснодар, Россия, pi_korolev@mail.ru

АННОТАЦИЯ

Цель исследования заключается в выработке методики формирования оптимального комплекса средств защиты информации на объектах критической информационной инфраструктуры, направленного на снижение риска реализации угрозы информационной безопасности.В этой связи, предметом исследования выступают требования к обеспечению информационной безопасности на объектах критической информационной инфраструктуры Российской Федерации.Исследована существующая нормативно-правовая база в области защиты информации в целом и организации ведомственного сегмента государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру, в частности. Сформулирован принцип проектирования оптимального состава средств указанной системы, основанный на применении связки «уязвимости-меры-средства защиты информации». Последовательное перекрытие каждого последующего звена связки предыдущим обеспечивает достижение надежности формируемого комплекса средств системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру. Формулировка ограничений базируется на полном перекрытии мерами всех уязвимостей, сформулированных в базе MITRE. Далее средствами – всех мер, отраженных в действующем приказе Федеральной службы по техническому и экспортному контролю России №239 от 25 декабря 2017 года «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Предполагается, что применение предложенной связки обеспечит снижение рисков реализации угроз информационной безопасности на объектах критической информационной инфраструктуры. Сформулирован и обоснован перечень ограничений, учитывающих специфику применения средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру, представлена целевая функция. Оптимизационная задача сведена к известной задаче целочисленного линейного программирования и может быть решена методами сечения Гомори, разветвления и прочими методами решения задач целочисленной оптимизации. Предложенная методика может использоваться на значимых объектах критической информационной инфраструктуры Российской Федерации для обеспечения соответствия действующим нормативным требованиям безопасности.

КЛЮЧЕВЫЕ СЛОВА: комплекс средств защиты информации; система обнаружения, предупреждения и ликвидации последствий компьютерных атак; база MITRE; оценка уязвимостей; меры защиты информации; совместимость средств защиты информации;оценки меры обеспечения безопасности.

Введение

Вопросы информационной безопасности приобретают особую актуальность по многим причинам. К их числу можно отнести данные Совета Безопасности Российской Федерации, согласно которым в 2016 году было совершено более 50 миллионов кибератак на информационные ресурсы Российской Федерации, более половины из которых было реализовано со стороны иностранных государств [1]. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [2].

Формирование рациональной подсистемы защиты информации (ЗИ) в автоматизированных системах предполагает наличие множества вариантов конфигураций, состоящих из множества средств ЗИ и дальнейший выбор из этого множества оптимального варианта построения комплекса средств ЗИ по определенным критериям [3].

Обеспечение ЗИ информационно-телекоммуникационных сетей (ИТКС) и информационных систем (ИС) значимых объектов критической информационной инфраструктуры Российской Федерации (КИИ) диктует необходимость учёта множества внутренних и внешних факторов влияющих на достаточный уровень защищенности. Преобразование характера угроз информационной безопасности (ИБ) затрудняет процесс решения задач должностными лицами органов системы обнаружения предупреждения и ликвидации последствий компьютерных атак (СОПКА). Этот аспект справедливо должен быть компенсирован таким комплексом средств защиты информации, который бы надежно перекрывал все возможные уязвимости с одной стороны и соответствовал действующим нормативным документам, регламентирующим меры обеспечения ИБ значимых объектов КИИ — с другой. Ограниченность ресурсов, в том числе материальных, непрерывное преобразование угроз информационной безопасности и связанные с этим сложности формируют соответствующую научно-техническую проблему и остро ее актуализируют.

Особенности проектирования оптимального состава
средств защиты информациив автоматизированных системах управления

Для дальнейшего решения задачи проектирования оптимального комплекса средств ЗИнеобходимо определить и обосновать круг особенностей, которые должны быть учтены при математической постановке задачи. К их числу относятся:

– перечень и оценка уязвимостей ИБ изложены и утверждены MITRE. Основание для использования данной базы продиктовано ее полнотой, оперативностью пополнения и отсутствием равноценной отечественной альтернативы;

– перечень технических мер обеспечения ИБ значимого объекта КИИдолжен в достаточной степени гарантироватьнейтрализацию всех уязвимостей базы MITRE. В данном случае под исчерпывающим перечнем технических мер будет пониматься состав мер по обеспечению ИБ для значимого объекта соответствующей категории значимости, установленный приказом ФСТЭК России № 239 от 25 декабря 2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– количество перекрытий одной и той же меры разными средствами ЗИ из комплекса должно быть минимальным. Это продиктовано стремлением к экономизации материальных

ресурсов. По данному критерию на рис. 1 отражена схема перекрытия мер двумя разными вариантами комплекса средств ЗИ.

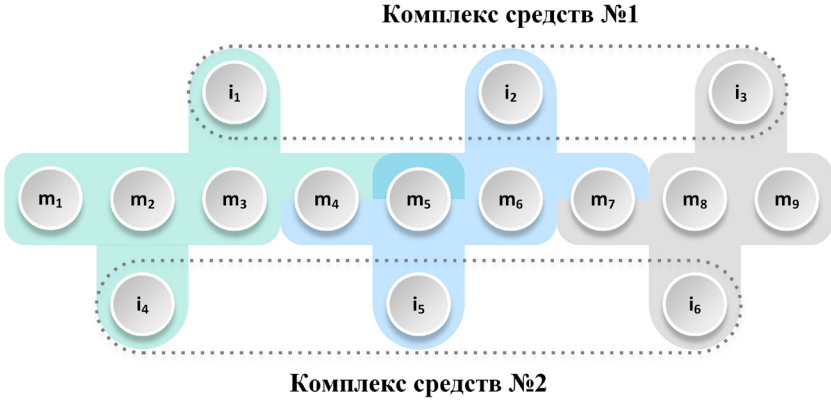

Рис. 1. Схема закрытия мер двумя разными вариантами комплекса средств ЗИ

В соответствии с данной схемой реализуется принцип выбора варианта комплекса, где предпочтительным будет тот комплекс, количество средств ЗИ, перекрывающих одни и те же меры, будет меньше;

– уязвимости из базы MITREдолжны быть полностью перекрыты мерами из указанного приказа ФСТЭК России, а последние должны быть в полном объеме перекрыты средствами ЗИ, входящими в формируемый комплекс;

– комплекс должен состоять из средств ЗИ с максимально высокими оценками. Определение оценки средства СОПКА заключается в нахождении отношения суммы оценок тех мер, которые оно закрывает, к сумме оценок всех мер, определенных приказом ФСТЭК России. Расчет данной оценки производится по формуле (1):

$$O_{ij} = \frac{\sum\limits_{m \in T} O_m}{\sum\limits_{i=1}^{n} O_{mi}}, \quad (1)$$

где T — меры, реализуемые средством ЗИ.

В свою очередь, для получения оценки меры необходимо найти значение отношения суммы оценок уязвимостей, которые данная мера перекрывает к сумме оценок всех уязвимостей, которые отражены в MITRE.

Так, оценка меры строится на количестве уязвимостей, которые нейтрализуются данной мерой, а также на критичности этих уязвимостей [4, 5]. Расчет производится по формуле (2):

$$O_{mi} = \frac{\sum\limits_{y_i \in p} O_y}{\sum\limits_{i=1}^{z} O_{yi}}, \quad (2)$$

где p — уязвимости, которые закрывает данная мера;

O_y — оценка уязвимости, определенная MITRE.

В табл. 1 и 2 отражен принцип формирования итоговой оценки средства ЗИ.

Таблица 1

Принцип расчета оценки меры обеспечения безопасности значимых объектов КИИ Российской Федерации

меры	оценка меры	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8	y_9	∑оценок
		1	3	5	7	9	2	4	6	10	
m_1	0,47	1	0	0	7	0	0	4	0	10	
m_2	0,26	0	3	0	0	9	0	0	0	0	**47**
...	0,55	0	0	5	0	9	2	0	0	10	
m_n	0,62	1	0	5	0	9	0	4	0	10	

*y – условное обозначение уязвимостей

Таблица 2

Принцип расчета оценки средств ЗИ

средства ЗИ	оценка	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}	m_{11}	m_{12}	∑ оценок
		0,5	0,3	0,5	0,3	0,6	0,4	0,7	0,4	0,4	0,3	0,4	0,6	
i_1	0,54	0,5	0,0	0,0	0,3	0,0	0,0	0,7	0,0	0,4	0,0	0,4	0,6	
i_2	0,21	0,0	0,3	0,0	0,0	0,6	0,0	0,0	0,0	0,0	0,3	0,0	0,0	**5,36**
...	0,43	0,0	0,0	0,5	0,3	0,0	0,4	0,7	0,4	0,0	0,0	0,0	0,0	
i_m	0,46	0,0	0,0	0,5	0,0	0,6	0,4	0,0	0,0	0,4	0,0	0,0	0,6	

– для технической реализации системы должно выполняться условие совместимости, которая производится в тех случаях, когда совместимость между подсистемами ЗИ предусмотрена [6]. Пример определения наличия или отсутствия связи между подсистемами ЗИ схематично представлен на рис. 2.

Заметим также, что одно средство ЗИ может входить в разные подсистемы ЗИ, при этом оно должно входить как минимум в одну подсистему ЗИ. Схематично приведенный подход представлен на рис. 3.

Численные значения критичности уязвимостей определены MITRE. Принцип расчета оценки средства ЗИ аналогичен тому, что представлен в табл. 1.

При наличии такой связи в формируемом варианте комплекса связь сохраняется и в отношении каждого элемента подсистем (средства ЗИ), входящего в указанные взаимосвязанные подсистемы ЗИ.

Заметим также, что одно средство ЗИ может входить в разные подсистемы ЗИ, при этом оно должно входить как минимум в одну подсистему ЗИ. Схематично приведенный подход представлен на рис. 3.

Рис. 2. Схема взаимосвязи между подсистемами ЗИ

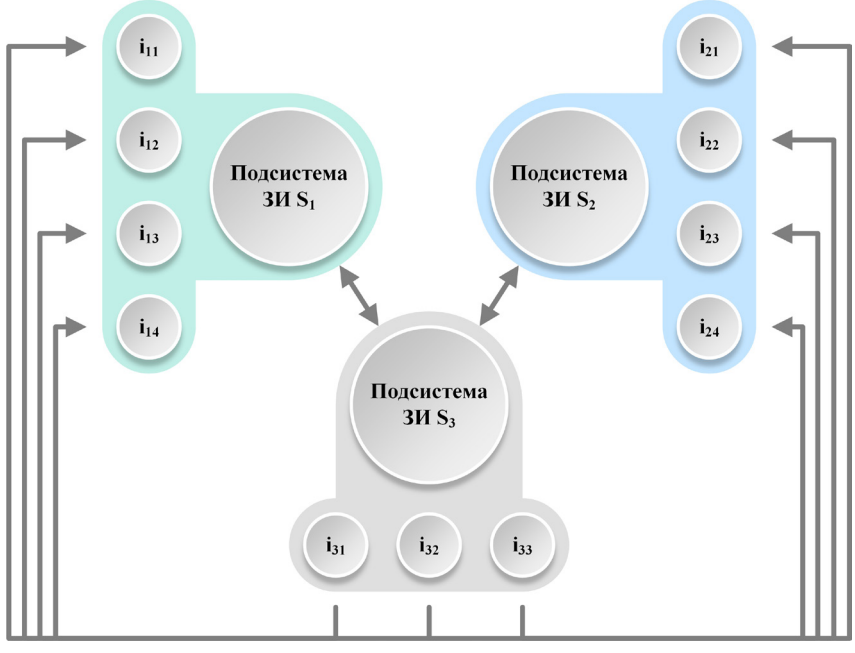

Рис. 3. Схема определения наличия связей между средствами ЗИ в зависимости от наличия связи между подсистемами ЗИ

Таким образом, этапы расчета совместимости комплекса выглядят следующим образом:

1. Определение схемы (шаблона) требуемых совместимостей подсистем ЗИкак граф [7, 8] $H = H(S)$, определяющий необходимые связи (ребра графа) $E = (S_i, S_j)$ между подсистемами ЗИ (вершины графа) $S_i, S_j \subset S$, $S = \{S_1 \ldots, S_i\}$. Каждому ребру $E = (S_i, S_j)$ графа поставим в соответствие вес $v(Si, Sj) = (v_1,\ldots, v_1)$, где $v_d \in \{v_1,\ldots, v_1\}$принимает значение 0 или 1, и равен 1, если между парой подсистем S_i, S_j требуется совместимость вида d. Иначе равен 0. Виды совместимости приведены в соответствии с ГОСТ 2.114–2016 «Единая система конструкторской документации. Технические условия. Правила построения, изложения и оформления», в том числе справедливы для средств ЗИ;

2. Оценка степени совместимости пары средств ЗИ, входящей в комплекс и относящейся к взаимосвязанным подсистемам ЗИ;

3. Установка факта перекрытия каждого из выделенных видов совместимости осуществляется на основании документации к соответствующему средству.В случае отсутствия такой информации, определение вида совместимости между соответствующими средствами СОПКА производится экспертным путем. Количество видов совместимости по каждому средству ЗИ вСОПКА должно устанавливаться персонифицировано в связи с особенностями его функционирования;

4. Определение общей оценки уровня совместимости средств ЗИ в комплексе путем заполнения матриц, пример которой представлен в табл. 3 и 4.

Таблица 3

Матрица весов графа $H=H(S)$ для пар подсистем ЗИ

Пары подсистем ЗИ	Требуемый вид совместимости										
	1	2	3	4	5	6	7	8	9	10	11
S_1S_2	0	0	0	0	1	1	1	0	0	0	1
S_1S_3	1	1	0	1	0	1	0	0	1	1	0
S_1S_4	0	1	0	0	0	0	0	1	0	1	0

Таблица 4

Матрица данных для расчета показателя уровня совместимости между средствами ЗИ, входящих в вариант комплекса

Возможные пары средств ЗИ	вид совместимости											Оценка $O(i_g i_q)$
	1	2	3	4	5	6	7	8	9	10	11	
i_1i_4	1	0	0	0	1	1	1	0	0	0	1	1
i_1i_7	1	0	0	0	1	0	1	0	1	0	0	0
i_1i_9	1	0	0	1	0	0	1	0	0	0	0	0
i_1i_{12}	0	0	1	1	1	0	0	0	0	0	0	0
i_2i_4	0	1	1	0	1	1	1	1	1	0	1	1
i_2i_7	1	1	0	1	1	1	1	0	1	1	0	1
i_2i_9	0	1	0	0	0	0	1	0	1	1	1	0
i_2i_{12}	1	1	1	0	1	0	0	1	0	1	1	1
i_1i_8	1	1	0	1	0	1	1	1	1	1	1	1
i_1i_{10}	0	1	1	1	1	1	0	1	0	1	0	1

Определение общей оценки уровня совместимости средств ЗИ в комплексе производится по формуле:

$$O_X = \min_{(S_i S_j)\in H} \max_{(i_g i_q)\in S_i \times S_j} O(i_g i_q)\cdot x_g \cdot x_q, \quad (3)$$

где максимальное значение выбирается из произведений оценок совместимостей всевозможных пар средств $i_g i_q$, которые берутся из декартового произведения соответствующих им подмножеств ЗИ $S_i \times S_j = \{(i_g i_q) \mid i_g \in S_i, i_q \in S_j\}$; минимальное значение берется по всем ребрам графа совместимостей Н.

– время развертывания системы должно лимитироваться в зависимости от периода и целей создания системы ЗИ и формирования оптимального комплекса средств ЗИ на значимом объекте КИИ. При определении времени развертывания используются два способа:

1) последовательное развертывание системы используется в случае осуществления развертывания минимальным количеством сил и необходимых хостовых объектов. При этом расчет должен производиться путем суммирования времени, необходимого для развертывания каждого элемента проектируемой системы;

2) параллельное развертывание системы используется в случае наличия увеличенного количества сил и ресурсов, необходимых для развертывания системы. В данном случае идет речь о применении превышающего количества ресурсов над количеством хостовых объектов. Расчет производится путем нахождения наибольшего значения времени на развертывание системы среди всех средств ЗИ, входящих в комплекс.

– должны быть определены пороговые значения стоимости формируемого комплекса средств ЗИ для значимого объекта КИИ в зависимости от ряда параметров, таких как: размер финансирования организации; масштаб организации и прочие затраты ресурсов [9]. Сюда же должны быть включены сопутствующие затраты на: возможное обучение/переобучение работников, связанное с установкой новых средств; покупку лицензий; платную техническую поддержку и другиезатраты, неотделимые от самого средства и без которых работоспособность данного средства ЗИ может быть поставлена под сомнение;

– количество средств ЗИ в комплексе должно стремиться к минимуму для сокращения степени риска, связанного с силами, требуемыми для управления и контроля над работоспособностью каждого средства ЗИ [10, 11].

Таким образом, по каждому пункту, отражающему особенности построения оптимального комплекса средств ЗИ дано краткое обоснование причин, по которым следует его учитывать при постановке и решении задачи оптимизации.

Математическая постановка задачи

Исходные данные:

1. $I = \{i_1,\ldots, i_k\}$ — множество всех средств ЗИ;

2. $M = \{m_1,\ldots, m_n\}$ — множество мер по приказу ФСТЭК России № 239 от 25 декабря 2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

3. $m_{ij} \in \{0;1\}$, $i = \overline{1,k}$, $j = \overline{1,n}$

$$m_{ij} = \begin{cases} 1 \\ 0, \end{cases}$$

1 — если *j*-я мера реализована в *i*-м средстве ЗИ;

0 — если *j*-я мера не реализована в *i*-м средстве ЗИ;

4. $S = \{S_1,\ldots, S_t\}$ — множество подсистем ЗИ, в свою очередь $S_1,\ldots, S_t$ являются подмножествами S, которые содержат определенное количество средств $\{i_1,\ldots, i_q\}$;

5. $c_i,\ i = \overline{1,k}$ — стоимость *i*-го средства ЗИ;

6. O_x — общая оценка совместимости комплекса средств ЗИ.

Введем булеву переменную $x_i \in \{0;1\},\ i = \overline{1,k}$, такую что:

$$x_i = \begin{cases} 1, \\ 0 \end{cases}$$

1 — если *i*-е средство ЗИ есть в решении;

0 — если *i*-го средства ЗИ нет в решении.

Тогда $X = (x_1,\ldots, x_k)$ — решение в виде вектора булевых переменных — комплекс средств ЗИ.

Учитывая особенности и требования при формировании оптимального комплекса средств СОПКА, целевая функция будет выглядеть следующим образом:

$$\sum_{j=1}^{n}\sum_{i=1}^{k} x_i m_{ij} \to \min$$

Смысл приведенной целевой функции заключается в том, чтобы минимизировать число так называемых пересечений мер несколькими средствами ЗИ одновременно.

Система ограничений выглядит следующим образом:

$$\begin{cases} \min\limits_{j=1,n}\sum\limits_{i=1}^{k} x_i m_{ij} \\ \sum\limits_{i=1}^{k} x_i \le x\ , x = \text{const} \\ \sum\limits_{i=1}^{k} O_{x_i} x_i \ge O, O = \text{const} \\ \sum\limits_{i=1}^{k} c_i x_i \le c, c = \text{const} \\ \sum\limits_{i=1}^{k} t_i x_i \le t, t = \text{const} \\ \mathrm{O_x} \ge 1 \end{cases}$$

Таким образом, решение задачи — нахождение всех неизвестных компонент вектора — *X* и выбор тех средств ЗИ из множества $I=\{i_1,\ldots, i_k\}$, для которых соответствующая компонента вектора x_i равна 1.

Данная оптимизационная задача сводится к известной задаче целочисленного линейного программирования, и может быть решена методами: сечения Гомори, разветвления[12] и т.д.

Заключение

Современное состояние проблемы проектирования оптимального состава комплекса средств ЗИ характеризуется наличием большого количества моделей, которые в большинстве основаны на вычислениях и имеют присущие такого рода вычислениям недостатки в условиях высокой неопределенности исходной информации [13].

Формирование научной задачи по построению оптимального комплекса средств ЗИ связано с введением в действие 26 июля 2017 г. Федеральногозакона № 187 «О безопасности критической информационной инфраструктуры», регулирующего отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Приказом № 239 от 25 декабря 2017 г. утверждены требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, однако четкого механизма, обеспечивающего меры, отраженные в данном приказе, не представлено. Предложенная методика проектирования оптимального комплекса средств ЗИ учитывает перекрытие множества мер, отраженных в упомянутом приказе. Кроме того, методикой предусмотрено использование базы уязвимостей MITRE, которая имеет наиболее широкий и регулярно пополняемый перечень уязвимостей с многокомпонентной оценкой их критичности, что позволяет дать оценку мере обеспечения безопасности, а также средства ЗИ, которая данную меру перекрывает. Последовательное взаимоувязывание уязвимостей с мерами; мер — со средствами ЗИ образовывает соответствующую триаду, схожую по структуре с моделью «угрозы-уязвимости-объекты защиты», сформулированную в [14].

Приведенная методика проектирования оптимального комплекса средств ЗИ для значимых объектов КИИ является частным случаем классической оптимизационной задачи. Формализация и обоснование особенностей применения средств ЗИ позволили сформулировать целевую функцию и соответствующие ограничения, что в конечном итоге существенно повышает эффективность составления комплекса средств ЗИ с точки зрения перекрытия всех уязвимостей и использования при этом всех мер, предусмотренных действующим законодательством.

Литература

1. *Хисамов Ф. Г., Шерстобитов Р. С.* Принципы формирования комплекса средств защиты информации при проектировании автоматизированных систем в защищенном исполнении // Материалы VIII Международной научно-технической конференции «Технологии разработки информационных систем» (Геленджик, 03–09 сентября 2017 г.). Геленджик, 2017. С. 71–76.

2. *Давыдов А. Е., Максимов Р. В., Савицкий О. К.* Защита и безопасность ведомственных и интегрированных инфокоммуникационных систем. М.: Воентелеком, 2017. 535 с.

3. *Баричев С. Г., Быков К. В.* Алгоритм оптимизации комплекса средств защиты информации канала передачи данных БПЛА // Материалы VII Международной научно-практической конференции «Современная наука: актуальные вопросы, достижения и инновации» (Пенза, 05 июня 2019 г.). Пенза, 2019. С. 56–59.

4. *Johnson L.* Computer Incident Response and Forensics. Rockland: Syngress, 2013. 259 p.

5. *Hamm, J., Ballenthin, W.* Threat Research. Incident Response with NTFS INDX Buffers. [FireEye] URL: https://www.fireeye.com/blog/threat-research/2012/09/striking-gold-incident-response-ntfs-indx-bufferspart-1.html (дата обращения 13.07.2020).

6. *Stauffer O, Barbosa V. C.* [A Study of the Edge-Switching Markov-ChainMethod for the Generation of Random Graphs]. Rio de Janeiro: Universidade Federaldo Rio de Janeiro, 2005. 156 p.

7. *B. Bollob´as, O. Riordan* [Mathematical results on scale-free random graphs]. Weinheim: Wiley-VCH, 2003. 34 p.

8. *Perez P. Velasco* Matrix Graph Grammars: An Algebraic Approach to GraphDynamics: VDM Verlag, 2009. 284 p.

9. *Паращук И. Б., Пащенко В. В*. Качество и надежность комплексов средств защиты информации для современных автоматизированных систем: показатели и критерии оценивания // Сборник трудов конференции «Региональная информатика и информационная безопасность» (Санкт-Петербург, 23–25 октября 2019 г.). 2019. С. 97–101.

10. *Бурмакина А. В., Рогозин Е.* С. Описание рациональной структуры комплекса программных средств защиты информации автоматизированных систем // Материалы Всероссийской научно-практической конференции «Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем» (Воронеж, 6 июня 2019 г.). Воронеж, 2019. С. 72–73.

11. *Tudor R*. The Global Information Network Architecture (GINA) Technology Framework. Naval Postgraduate School URL: http://www.emacoe.org/LinkClick.aspx?link=http://files.me.com/ bktech/8zhx34&tabid=60&mid=378 (дата обращения 13.07.2020).

12. *Achlioptas D, Clauset A., Kempe D., Moore C.* On the bias of traceroute sampling: or, power-law degree distributions in regular graphs // In Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, 2005. Pp. 694–703.

13. *Дидрих В. Е., Паладьев В.* В. Модель рационального распределения элементов комплекса средств защиты информации по элементам информационной системы // Актуальные направления научных исследований XXI века: теория и практика. 2015. № 7. С. 76–80.

14. *Винокуров А. В*. Модель системы защиты информации и контроля целостности критически-важных систем робототехнических комплексов от внешних деструктивно-информационных воздействий // Материалы конференции «Перспективные методы и средства защиты информационной инфраструктуры» (Анапа, 17 апреля 2019 г.). Анапа, 2019. С. 67–74.

MATHEMATICAL OPTIMIZATION OF INFORMATION PROTECTION SYSTEM IN AUTOMATED CONTROL SYSTEMS

RODION M.PASECHNIK,
senior researcher of Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia, rmpasechnik@mail.ru

MARINA P. TABUNKOVA,
senior researcher of Krasnodar Higher Military Schoo named after General of the Army S. M. Shtemenko, Krasnodar, Russia, skygel@mail.ru

IGOR D. KOROLEV,
senior researcher of Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, Krasnodar, Russia, pi_korolev@mail.ru

ABSTRACT

The purpose of the study is to develop a methodology for compiling an optimal set of information protection tools at critical information infrastructure facilities aimed at reducing the risk of implementing an information security threat. In this regard, the subject of the study is the requirements for ensuring information security at critical information infrastructure facilities of the Russian Federation. The existing regulatory The legal framework in the field of information protection in general and the organization of the departmental segment of the state system for detecting, preventing and eliminating the consequences of computer attacks on critical information infrastructure, in particular. The principle of designing the optimal composition of the tools of the specified system is formulated, based on the use of a combination of «vulnerability – measures – information protection means». Sequential overlapping of each subsequent link of the ligament with the previous one ensures achievement of reliability of the formed complex of tools for the system of detection, prevention and elimination of the consequences of computer attacks on critical information infrastructure. The wording of the restrictions is based on the complete overlapping measures of all the vulnerabilities formulated in the MITRE database. Further, by means of all measures reflected in the current order of the Federal Service for Technical and Export Control of Russia No. 239 dated December 25, 2017 «On the Approval of the Requirements for the Safety of Important Critical Information Infrastructure Facilities of the Russian Federation». It is assumed that the use of the proposed bundle will reduce the risks of the implementation of information security threats at the critical information infrastructure facilities. A list of other restrictions is formulated and justified, taking into account the specifics of using the means of the state system for detecting, preventing and eliminating the consequences of computer attacks on critical information infrastructure, the objective function is presented. The optimization problem is reduced to the well-known integer linear programming problem and can be solved by the methods of Gomori section, branching and other methods of solving integer optimization problems. The proposed methodology can be used at significant facilities of the critical information infrastructure of the Russian Federation to ensure compliance with current regulatory safety requirements.

Keywords: a set of information security tools; system for detecting; preventing and eliminating the consequences of computer attacks; MITRE database; vulnerability assessment; information security measures; information security compatibility; security measures assessment.

REFERENCES

1. Hisamov F. G., Sherstobitov R. S. Principy formirovanija kompleksa sredstv zashhity informacii pri proektirovanii avtomatizirovannyh sistem v zashhishhennom ispolnenii [The principles of the formation of a set of information protection tools in the design of automated systems in a secure execution]. *Materialy VIII Mezhdunarodnoj nauchno-tehnicheskoj konferencii "Tehnologii razrabotki informacionnyh system"* [Proceedings of the VIII international scientific-technical conference "Designs technologies of information system", Gelendzhik, on September 03–09, 2017]. Gelendzhik, 2017. Pp. 71–76. (In Rus)
2. Davydov A. E., Maksimov R. V., Savickij O. K. *Zashhita i bezopasnost' vedomstvennyh i integrirovannyh infokommunikacionnyh system* [Protection and security of departmental and integrated information and communication systems]. Moscow: OAO «Voentelekom», 2017. 535 p. (In Rus)
3. Barichev S. G., Bykov K. V. Algoritm optimizacii kompleksa sredstv zashhity informacii kanala peredachi dannyh BPLA [Optimization algorithm of the protection means complex of information of the UAV data channel]. *Materialy VII Mezhdunarodnoj nauchno-prakticheskoj konferencii "Sovremennaja nauka: aktual'nye voprosy, dostizhenija i innovacii"* [Proceedings of the VII international scientific-practical conference "Modern science: topical questions, progress and innovation", Penza, on June 05, 2019]. Penza, 2019. Pp. 56–59. (In Rus)
4. Johnson L. *Computer Incident Response and Forensics*. Rockland: Syngress, 2013. 259 p.
5. Hamm J., Ballenthin W. Threat Research. Incident Response with NTFS INDX Buffers. [FireEye] URL: https://www.fireeye.com/blog/threat-research/2012/09/striking-gold-incident-response-ntfs-indx-bufferspart-1.html (date of access 13.07.2020).
6. Stauffer O., Barbosa V. C. *A Study of the Edge-Switching Markov-ChainMethod for the Generation of Random Graphs*. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2005. 156 p. (In Portuguese)
7. Bollob´as B., Riordan O. *Mathematical results on scale-free random graphs*. Weinheim: Wiley-VCH, 2003. 34 p.
8. Perez P. *Velasco Matrix Graph Grammars: An Algebraic Approach to Graph Dynamics*. Verlag: VDM, 2009. 284 p.
9. Parashhuk I. B., Pashhenko V. V. Kachestvo i nadezhnost' kompleksov sredstv zashhity informacii dlja sovremennyh avtomatizirovannyh sistem: pokazateli i kriterii ocenivanija [Quality and reliability of complexes of information protection means for modern automated systems: indicators and criteria of evaluation]. *Materialy konferencii "Regional'naja informatika i informacionnaja bezopasnost'"* [Proceedings of the conference "Local informatics and information security", Saint-Petersburg, on October 23–25, 2019]. Saint-Petersburg, 2019. Pp. 97–101. (In Rus)
10. Burmakina A. V., Rogozin E. S. Opisanie racional'noj struktury kompleksa programmnyh sredstv zashhity informacii avtomatizirovannyh sistem [Description of the rational structure of the complex of software means for protecting information of automated systems]. *Materialy V serossijskoj nauchno-prakticheskoj konferencii "Aktual'nye voprosy jekspluatacii system ohrany i zashhishhennyh telekommunikacionnyh system"* [Proceedings of the IV all-Russian scientific-practical conference "Topical questions of system maintenance of protection and protected telecommunication network", Voronezh, on June 06, 2019]. Voronezh, 2019.Pp. 72–73. (In Rus)
11. Tudor R. The Global Information Network Architecture (GINA) Technology Framework. Naval Postgraduate School URL: http://www.emacoe.org/LinkClick.aspx?link=http://files.me.com/ bktech/8zhx34&tabid=60&mid=378 (date of access 13.07.2020).
12. Achlioptas D, Clauset A., Kempe D., Moore C. On the bias of traceroute sampling: or, power-law degree distributions in regular graphs. *In Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, 2005. Pp. 694–703.
13. Didrih V. E., Palad'ev V. V. Model of rational distribution of elements of complex of means of protection of information on elements of information system. *Aktual'nye napravlenija nauchnyh issledovanij XXI veka: teorija i praktika* [Topical lines of investigationof scientific researchXXI: theory and practice]. 2015. No. 7. Pp. 76–80. (In Rus)
14. Vinokurov A. V. Model' sistemy zashhity informacii i kontrolja celostnosti kriticheski-vazhnyh system robototehnicheskih kompleksov ot vneshnih destruktivno-informacionnyh vozdejstvij [Information protection system model and integrity control of critical and important systems of robotic complexes from external destructive information influences]. *Materialy konferencii "Informacionnaja bezopasnost"* [Proceedings of the conference «Information security», Anapa, on April 17]. Anapa, Pp. 67–74. (In Rus)