http://dx.doi.org/10.35596/1729-7648-2023-21-2-95-103

Оригинальная статья
Original paper

УДК 004.056

МОДЕЛЬ И МЕТОД ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНОЙ СТРУКТУРЫ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В. А. КАСУМОВ, ДЖ. И. МАМЕДОВ

Азербайджанский технический университет (г. Баку, Республика Азербайджан)

Поступила в редакцию 19.12.2022

Аннотация. Исследована проблема информационной безопасности критических информационных инфраструктур. Проанализированы особенности критически важных объектов с точки зрения сбора, обработки, хранения и передачи информации. Изучены совокупность функций, выполняемых системой обеспечения безопасности информации в критических инфраструктурах, и зависимости между этими функциями. Предложена модель системы обеспечения безопасности и определены требования, предъявляемые к ней. Множество отношений между объектами и угрозами представлено в виде графа отношений «объект – угроза», в котором ребро, связывающее *j*-й объект с *i*-й угрозой, существует только тогда, когда *i*-я угроза может воздействовать напрямую на *j*-й объект. Для защиты объектов критических информационных инфраструктур от возможных угроз в модель системы обеспечения безопасности введено множество необходимых методов и средств, преобразующее двухдольный граф в трехдольный, типа «объект – метод – угроза». Рассмотрена задача определения оптимальной структуры системы обеспечения безопасности объектов критической информационной инфраструктуры, решение которой позволит свести к минимуму материальные затраты на реализацию средств защиты и ущерб от нарушения безопасности.

Ключевые слова: критические инфраструктуры, защита информации, модель системы безопасности, угрозы, граф отношений, ущерб от нарушения, оптимальная структура системы.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Касумов, В. А. Модель и метод определения оптимальной структуры системы обеспечения безопасности для критической информационной инфраструктуры / В. А. Касумов, Дж. И. Мамедов // Доклады БГУИР. 2023. Т. 21, № 2. С. 95–103. http://dx.doi.org/10.35596/1729-7648-2023-21-2-95-103.

MODEL AND METHOD FOR DETERMINING THE OPTIMAL STRUCTURE OF THE SECURITY SYSTEM FOR CRITICAL INFORMATION INFRASTRUCTURE

VAGIF A. GASIMOV, JABIR I. MAMMADOV

Azerbaijan Technical University (Baku, Republic of Azerbaijan)

Submitted 19.12.2022

Abstract. The article investigates the problem of information security of critical information infrastructures. The features of critical objects from the point of view of collecting, processing, storing and transmitting information are analysed. The set of functions performed by the information security system in critical infrastructures and the dependencies between these functions are studied. A model of the security system is proposed and the require-

ments for this model are defined. At the same time, the set of relations between objects and threats is represented in the form of an object-threat relationship graph, in which an edge connecting the *j*-th object with the *i*-th threat exists only when the *i*-th threat can directly affect the *j*-th object. To protect objects of critical information infrastructures from possible threats, a set of necessary methods and tools has been introduced into the model of the security system, which converts a two-sided graph into a three-sided one, such as "object – method – threat". Further in the article, the problem of determining the optimal structure of the security system for critical information infrastructure objects is considered. It is assumed here that each threat can affect several objects, and that any object can be affected by more than one threat. The solution of this problem makes it possible to minimize the material costs to implement the methods and tools for protection and minimize damage from a security breach.

Keywords: critical infrastructures, information protection, security system model, relationship graph, damage from breach, optimal system structure.

Conflict of interests. The authors declare no conflict of interests.

For citation. Gasimov V. A., Mammadov J. I. Model and Method for Determining the Optimal Structure of the Security System for Critical Information Infrastructure. *Doklady BGUIR*. 21 (2), 95–103. http://dx.doi.org/10.35596/1729-7648-2023-21-2-95-103 (in Russian).

Введение

Обеспечение безопасности критических инфраструктур является актуальной научной и практической задачей, так как их выход из строя приводит к нарушению работы всех сфер государственных структур. Статистика инцидентов в разных странах показывает, что угрозы, реализуемые по отношению к критическим инфраструктурам, в основном направлены на их информационные системы. В связи с этим обеспечение безопасности указанных систем должно являться приоритетным направлением обеспечения безопасности критических инфраструктур.

В настоящее время существует множество отдельных методов и средств обеспечения безопасности информационных систем. Но основной проблемой для специалистов является выбор наиболее эффективных из них для предотвращения угрозы информационной системе в конкретных случаях. В [1] представлено исследование, в результате которого изучены модели и методы создания эффективной системы обеспечения безопасности (СОБ) информации для распределенных компьютерных сетей, определена зависимость между потерями от угроз и стоимостью самой системы. Рекомендовано построить такую СОБ, структура которой являлась бы оптимальной, охватывала все возможные методы и средства обеспечения безопасности, но стоимость не превышала бы суммарный объем возможных потерь. Для этого была поставлена задача оптимизации, чтобы ее решение дало средневзвешенную величину ущерба (временных и материальных затрат) от нарушения безопасности системы в целом. Однако следует отметить, что в указанной модели не учитываются мероприятия и затраченные на них средства по ликвидации последствий реализованных угроз.

Авторами данной статьи исследована задача оптимизации структуры системы обеспечения безопасности информации в критических информационных инфраструктурах (КИИ). При этом учитывались особенности системы, указанные в [1]. Критическая инфраструктура – термин, используемый правительствами для описания активов, которые необходимы для функционирования общества и экономики страны. Другими словами, критическая инфраструктура – это объекты инфраструктуры, системы, их части и их совокупность, которые важны для экономики, национальной безопасности и обороны, нарушение функционирования которых может нанести вред жизненно важным национальным интересам.

Критически важный объект – это объект, нарушение и приостановление деятельности которого приводит к утрате управления экономикой страны, государственного субъекта, административно-территориальной единицы, либо к снижению безопасности жизнедеятельности населения [2][1]. Критическая информационная инфраструктура представляет собой совокупность автоматизированных систем управления технологическими и производственными процессами критических объектов и обеспечивает их взаимодействие с информационно-телекоммуникационными сетями, а также коммуникационными сетями и информационными системами, предназначенными для обеспечения государственного управления, обороноспособности и безопасности.

[1] Concepts, Classification and Regulation of Critical Information Infrastructure. https://rutlib5.com/book/27296.

Системы обработки информации обычно состоят из локальных сетей и отдельных компьютеров, которые распределены и взаимодействуют друг с другом с точки зрения данных и управления. Для сбора, обработки, хранения и передачи информации основными характеристиками систем обработки информации критических инфраструктурных объектов (КИО) являются следующие [3]:

– территориальная разбросанность компонентов системы и наличие между ними интенсивного информационного обмена;

– широкий спектр использования, хранения и передачи информации, а также методов описания;

– агрегирование данных разного назначения, принадлежащих различным субъектам, в рамках единой базы данных и, наоборот, размещение данных, необходимых тем или иным субъектам, в разных удаленных узлах сети;

– изоляция владельцев данных от физических структур и местонахождения данных;

– использование распределенных режимов обработки данных;

– участие большого количества пользователей и различных категорий персонала в автоматизированной обработке информации;

– одновременный и прямой доступ к информационным ресурсам большого количества различных категорий пользователей;

– высокий уровень разнообразия используемой компьютерной техники и средств связи, а также их программного обеспечения;

– отсутствие специальной аппаратной защиты у большинства основных технических средств, широко используемых в системе.

Анализ этих особенностей позволяет заблаговременно выявлять слабые места информационных систем КИО, угрозы безопасности, оценивать и управлять рисками, а также принимать защитные меры в соответствии с уровнями риска. Наличие вышеперечисленных особенностей создает условия для реализации многих естественных и искусственных угроз на информационные системы КИО. К таким угрозам можно отнести нарушение работы информационной системы КИО и средств ее защиты, несанкционированный доступ к системе и информационным ресурсам, изоляцию законных пользователей. Кроме того, такие угрозы, как нарушение работы, вызванные некомпетентным использованием охранных устройств обслуживающим персоналом, изменением их параметров и самовольным отключением, ошибочной отправкой данных на другой адрес, вводом неверных данных, неосознанным заражением системы компьютерными вирусами и т. п.

Как уже отмечалось, сегодня существует множество отдельных методов и средств защиты информации от тех или иных угроз, предназначенных для защиты, по крайней мере, одного объекта от одной угрозы, т. е. для противостояния одной угрозе. Но даже достаточно надежные методы и средства, разработанные и используемые автономно, не способны должным образом защищать объекты от угроз и исключать слабые (легко уязвимые) места в системе защиты данных. Отсюда можно сделать вывод, что безопасность данных может быть обеспечена и поддержана комплексом программных, аппаратных и организационных методов и средств защиты, которые выполняют свои функции в тесном взаимодействии с основными компонентами КИИ. Другими словами, для надежного решения проблемы обеспечения информационной безопасности требуется разработка хорошо организованной, эффективно действующей СОБ, основными задачами которой являются выбор эффективной структуры системы, упорядочивание функций общесистемных средств информационной безопасности, синтез структуры компонентов, оценка надежности защиты информации и т. д.

Следует отметить, что при разработке архитектуры СОБ для критически важных информационных инфраструктур особое внимание необходимо уделять проектированию и реализации общесистемных средств защиты. От их удачного проектирования во многом зависят такие характеристики, как надежность, отказоустойчивость и настраиваемость системы, мобильность и реализуемость программно-технических средств, стоимость и удобство эксплуатации, затраты на реализацию средств защиты, материальные и временные ущербы от нарушения безопасности. Перечисленные характеристики ставят свои требования к системе обеспечения безопасности и, следовательно, степенью предъявления этих требований определяется ее сложность.

Наиболее эффективными СОБ являются те, в которых реализованы все возможные и доступные методы и средства – как инженерно-технические, так и нетехнические. Однако реализация такого комплекса далеко не всегда может привести к желаемому результату. При этом следу-

ет учитывать, что ущерб от нарушения безопасности защищаемой информации или от различных несанкционированных действий может быть гораздо меньше стоимости СОБ (т. е. расходов на создание такой системы). Поэтому задача исследования и разработки экономически оптимальных СОБ, обеспечивающих наименьший риск владельцу и пользователям информации от ущерба и потерь в результате несанкционированных действий, является актуальной. В качестве основных параметров создания оптимальной СОБ можно рассмотреть ожидаемые суммарные потери и расходы в процессе защиты информации в течение определенного периода времени [4]. Исследования авторов статьи направлены на решение вопросов создания эффективной структуры СОБ, предназначенной для выполнения функций управления комплексом средств обеспечения безопасности данных, анализа риска и состояния системы, определения и оценки видов угроз, а также применения средств противодействия выявленным угрозам в КИИ.

Функциональное описание и модель системы обеспечения безопасности объектов критической информационной инфраструктуры

Основными задачами, подлежащими решению при обеспечении информационной безопасности в КИИ, являются [5]:

– оценка потенциально возможного ущерба от нарушения информационной безопасности объектов КИИ;

– формирование более полного перечня угроз объектам КИИ информационной безопасности и определение их характеристик;

– разработка методологии определения и прогнозирования значений характеристических показателей информационной безопасности объектов КИИ;

– определение политики безопасности КИИ;

– исследование и разработка системы решений, обеспечивающих информационную безопасность объектов КИИ беспрерывно;

– исследование и разработка способов, методов и средств эффективной реализации решений задач информационной безопасности;

– формирование системы условий, необходимых для эффективной реализации решений задач информационной безопасности или способствующих повышению их эффективности.

При организации работ по обеспечению информационной безопасности рекомендуется соблюдать следующие основные принципы:

– обеспечение безопасности информации в КИИ должно быть непрерывным процессом, заключающимся в систематическом контроле защищенности, выявлении узких и слабых мест, обосновании и реализации наиболее рациональных путей совершенствования и развития СОБ;

– безопасность информации в КИИ может быть обеспечена лишь при комплексном использовании и взаимодействии всего арсенала имеющихся средств защиты;

– никакая СОБ не способна обеспечить безопасность информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты;

– никакую СОБ нельзя считать абсолютно надежной, другими словами, следует учитывать, что может найтись такой умелый злоумышленник, который отыщет лазейку для доступа к информации.

Система обеспечения безопасности в КИИ является самым верхним в системной иерархии компонентом и в соответствии с отмеченными выше задачами должна выполнять следующие функции [5]: управление входом пользователей в систему, контроль доступа к системе и ее ресурсам, регистрация входов и обращений к системе, установление подлинности (аутентификация) пользователя и системы, контроль полномочий и привилегий пользователей, защита конфиденциальности информации, управление ключами (паролями) пользователей, обеспечение целостности и удостоверение подлинности данных, анализ состояния и контроль угроз, предотвращение нарушений в системе, реконфигурация системы обеспечения безопасности. Функции, выполняемые СОБ, в зависимости от ее структуры могут иметь следующие взаимоотношения между собой: могут выполняться независимо друг от друга, могут быть выполнены в строгой последовательности, выполнение одной функции может быть согласовано с другими функциями (даже со всеми), выполнение одной функции может вызывать выполнение других, выполнение одной функции может запретить выполнение других и даже потребовать отмены выполняемых.

Рассмотрим модель СОБ объектов КИИ. В целом КИИ – это совокупность информационных систем и телекоммуникационных сетей, критически важных для работы ключевых сфер жизнедеятельности государства и общества. Информационные системы объектов КИИ объединены телекоммуникационными сетями передачи данных, могут быть представлены в виде множества информационных ресурсов и прикладных процессов, которые для выполнения своих функций используют сетевые и системные ресурсы КИИ. В качестве ресурсов КИИ могут быть серверы, сервисные функции, базы данных или файлы в компьютере, информация, расположенная на носителе информации, устройства, подключенные к системе КИИ, процесс, выполняющийся в системе КИИ, и т. п. При этом все ресурсы могут быть разделены на активные, для выполнения собственных функций использующие другие ресурсы КИИ, и пассивные, участвующие при выполнении каких-либо функций под управлением активных ресурсов. Необходимо отметить, что ресурс может быть пассивным в один момент времени и активным в другой. Все ресурсы системы в дальнейшем назовем объектами КИИ.

Средства обеспечения безопасности данных можно разделить на два основных класса: локальные и распределенные средства защиты. Локальные средства защиты информации являются принадлежностью систем или сетей отдельных объектов КИИ и выполняют проверку возможности доступа пользователей и других к запрашиваемым ресурсам. Распределенные средства защиты информации обеспечивают управление потоками защищаемых данных в географически распределенных объектах КИИ и выполняют свои функции в тесном взаимодействии с сетевыми протоколами управления обработки и передачи данных.

СОБ должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему или доступа к объектам КИИ. В модели СОБ точно определяются все области, требующие защиты, оцениваются средства обеспечения безопасности с точки зрения их эффективности и их вклад в обеспечение безопасности во всей сетевой среде КИИ. Предполагается, что несанкционированный доступ к каждому из наборов защищаемых объектов сопряжен с некоторой величиной ущерба для своего владельца при нарушении безопасности. Также для ликвидации последствий совершенных угроз и полного восстановления работы программно-технических и информационных систем объектов КИИ требуются определенные материальные затраты.

В модели СОБ с каждым объектом КИИ, требующим защиты, связывается некоторое множество злоумышленных действий, т. е. угроз. В качестве набора угроз $T = \{t_j\}, j = \overline{1,J},$ направленных на нарушение безопасности, можно перечислить все потенциальные злоумышленные действия по отношению ко всем объектам $O = \{o_i\}, i = \overline{1,I}$ КИИ. Основной характеристикой набора угроз является $P = \|p_{ij}\|_{I \times J}$ – вероятность или частота появления угрозы t_j относительно объекта o_i [6, 7].

Множество отношений между объектами и угрозами можно представить в виде графа отношений «объект – угроза» (рис. 1), в котором ребро (t_j, o_i) существует тогда и только тогда, когда угроза t_j может воздействовать напрямую на объект o_i.

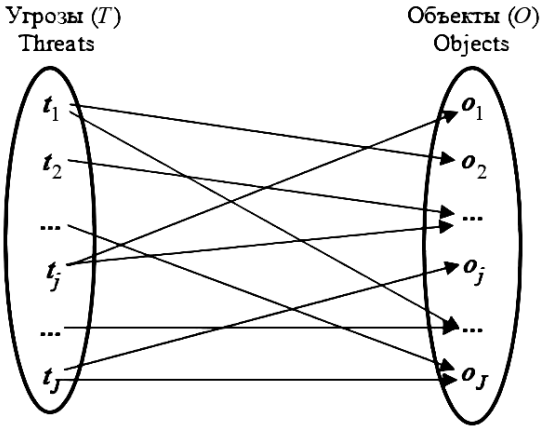

Рис. 1. Граф отношений «объект – угроза» базовой модели
Fig. 1. Graph of relations “object – threat” of the base model

Как видно из рисунка, связь между угрозами и объектами не является типа «один к одному». Другими словами, угроза может оказать воздействие на любое число объектов, а также на любой объект может воздействовать более чем одна угроза. Суть обеспечения информационной безопасности КИИ состоит в том, чтобы исключить все ребра графа типа (t_j, o_i) или свести к минимуму их количества, указывающие пути доступа угроз t_j на объекты o_i. Для этого в модель отношений «объект – угроза» вводится множество методов и средств защиты $M = \{m_1, m_2, \ldots, m_K\}$, которое должно обеспечивать безопасность всех объектов КИИ. Каждое средство m_k этого множества должно противостоять хотя бы одной угрозе, т. е. устранять хотя бы одно ребро (t_j, o_i) из заданного графа.

Таким образом, включение набора методов и средств обеспечения безопасности $M = \{m_1, m_2, \ldots, m_K\}$ преобразует двухдольный граф в трехдольный (рис. 2). Другими словами, в защищаемой системе все ребра типа (t_j, o_i) разбиваются на две части и представляются в форме (t_j, m_k) и (m_k, o_i).

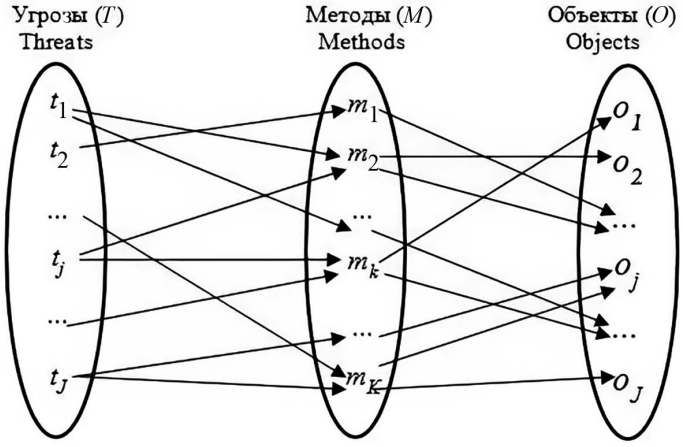

Рис. 2. Граф отношений «объект – метод – угроза» базовой модели
Fig. 2. Graph of relations "object – method – threat" of the base model

Понятно, что существование ребра типа (t_j, o_i) указывает незащищенность объекта o_i. Следует отметить, что отсутствие ребра (t_j, o_i) не гарантирует полную безопасность объекта o_i, хотя наличие такой связи дает потенциальную возможность существования угрозы, за исключением случая, когда вероятность появления ее равна нулю. Учитывая вышесказанное, базовую систему СОБ для КИИ можно представить следующим образом:

$$S = \{O, T, M, V, B\}, \tag{1}$$

где $O = \{o_1, o_2, \ldots, o_I\}$ – множество защищаемых объектов (информационных, технических и иных ресурсов) КИИ; $T = \{t_1, t_2, \ldots, t_J\}$ – множество злоумышленных действий (угроз), нарушающих безопасность объектов КИИ; $M = \{m_1, m_2, \ldots, m_K\}$ – множество методов и средств обеспечения безопасности защищаемых объектов КИИ; $V = \{v_1, v_2, \ldots, v_J\}$ – множество уязвимых мест в объектах КИИ, используемых угрозами, т. е. отображения типа $T \times O$ на множество упорядоченных $v_j = (t_j, o_i)$, представляющих собой пути проникновения угрозы t_j в объект o_i; $B = \{b_1, b_2, \ldots, b_I\}$ – множество «защитных барьеров», реализуемых для объекта o_i, т. е. отображение типа $V \times M$ или $T \times O \times M$ на набор упорядоченных троек $b_i = (t_j, o_i, m_k)$, представляющих собой точки, в которых требуется осуществлять защиту в КИИ [3].

На рис. 3 представлена функциональная схема модели (1), которая показывает отношения между объектами КИИ, угрозами и СОБ. Из рис. 3 видно, что угрозы могут получить доступ к объектам КИИ, только пройдя «защитные барьеры», образующиеся методами и средствами СОБ. Понятно, что максимальный уровень эффективности защитных барьеров достигается только тогда, когда для предотвращения угроз будут выбраны наиболее подходящие методы, средства или меры обеспечения безопасности.

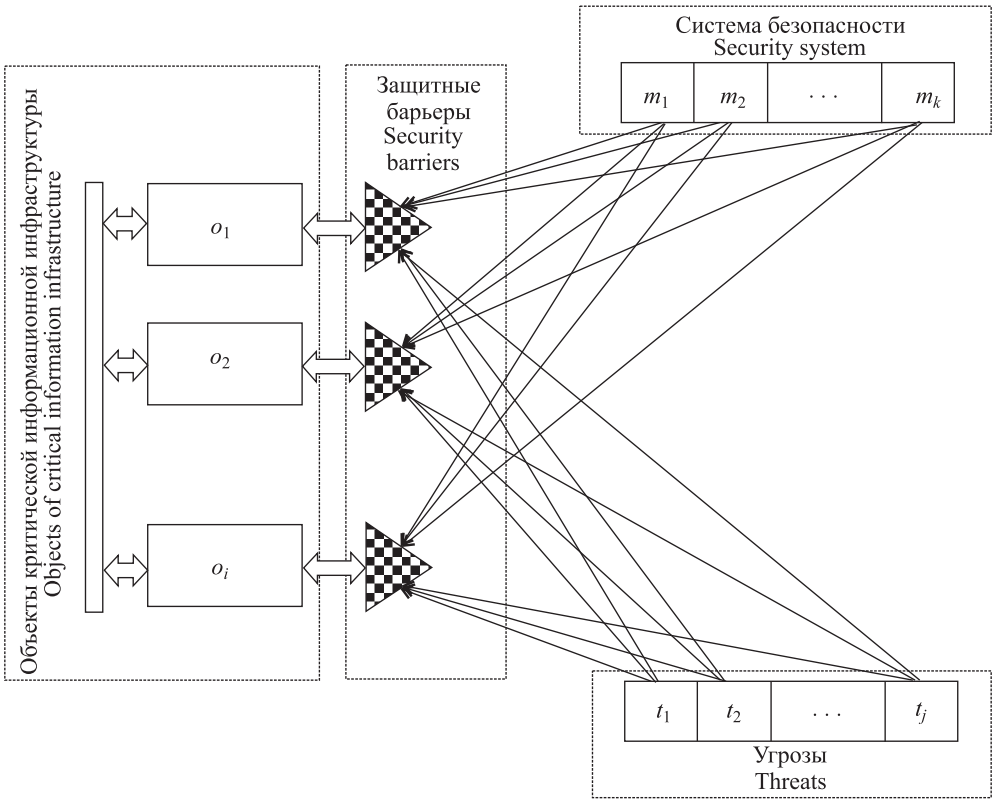

Рис. 3. Функциональная схема процесса информационной безопасности объектов критических инфраструктур
Fig. 3. Functional diagram of the process of information security of critical infrastructure objects

Модель оптимальной структуры системы обеспечения безопасности

Пусть в рамках модели (1) даны:

– $P = \left\| p_{ij} \right\|_{I \times J}$, где p_{ij} – вероятность или частота появления угрозы t_j относительно объекта o_i;

– $Z = \left\| z_{ij} \right\|_{I \times J}$, где z_{ij} – материальные расходы, требуемые для реализации необходимых методов и средств обеспечения безопасности объекта o_i от угрозы t_j;

– $Z' = \left\| z'_{ij} \right\|_{I \times J}$, где z'_{ij} – затраты, требуемые для устранения последствий угрозы t_j, причиненной объекту o_i;

– $Q = \left\| q_{ij} \right\|_{I \times J}$, где q_{ij} – материальный ущерб, наносимый в результате нарушения безопасности объекта o_i угрозой t_j;

– $X = \left\| x_{ijk} \right\|_{I \times J \times K}$, где $x_{ijk} = 1$, если объект o_i защищается с помощью средства защиты m_k от воздействие угрозы t_j, $x_{ijk} = 0$ – в противном случае.

Таким образом, задача определения оптимальной структуры системы обеспечения безопасности сводится к нахождению таких x_{ijk}, $i = \overline{1,I}$, $j = \overline{1,J}$, $k = \overline{1,K}$, которые минимизировали бы функционал

$$\sum_{i=1}^{I} \sum_{k=1}^{K} \sum_{j=1}^{J} p_{ij} \left(z_{ij} + z'_{ij} + q_{ij} \right) x_{ijk} \to \min \tag{2}$$

и удовлетворяли условиям:

$$\sum_{i=1}^{I} \sum_{j=1}^{J} \left(z_{ij} + z'_{ij} \right) \le Z_{\max}; \tag{3}$$

$$\sum_{k=1}^{K} x_{ij} \ge 1, i = \overline{1,I}; \tag{4}$$

$$\sum_{j=1}^{J} x_{ij} \geq 1, k = \overline{1, K}. \quad (5)$$

Функционал (2) показывает средневзвешенную величину материальных затрат на реализацию средств защиты и ущерба от нарушения безопасности объектов КИИ в целом. Условие (3) ограничивает объем общих затрат ($\leq Z_{max}$), требуемых для реализации необходимых методов и средств обеспечения информационной безопасности объектов КИИ и для ликвидации последствий угроз, (4) показывает, что каждый объект должен быть защищен хотя бы одним методом или средством защиты, а (5) – что каждый метод должен противостоять как минимум одной угрозе.

Заключение

1. В результате исследований моделей и методов создания эффективной системы обеспечения безопасности для критической информационной структуры определена зависимость между потерями от угроз и стоимостью самой системы безопасности. Выяснено, что разработка всеобъемлющей системы обеспечения безопасности, стоимость которой намного выше, чем объем возможных потерь, не всегда приемлема (исключение – информационная безопасность в области национальной и государственной безопасности).

2. Предложена такая система обеспечения безопасности, структура которой является оптимальной, охватывает необходимые методы и средства обеспечения безопасности, но стоимость ее не превышает суммарный объем возможных потерь. Для этого решена задача оптимизации, которая дает средневзвешенную величину материальных затрат на разработку и реализацию методов и средств системы обеспечения безопасности и ущерба от нарушения безопасности системы в целом. При этом объем общих затрат, требуемых для реализации необходимых методов и средств обеспечения информационной безопасности объектов критической информационной структуры и для ликвидации последствий угроз, должен быть ограничен сверху, каждый объект – защищен, по крайней мере, одним средством защиты, а каждый метод должен противостоять хотя бы одной угрозе.

Список литературы

1. Development of the Information Security System Effective Structure for the Distributed Computer Networks / V. A. Gasimov [et al.] // IOP Conf. Series: Materials Science and Engineering. 2019. Vol. 537. https://iopscience.iop.org/article/10.1088/1757-899X/537/5/052034/pdf.
2. Knapp, E. Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid SCADA, and Other Industrial Control Systems. 2nd ed. / E. Knapp, J. Langill. Syngress Publ., 2014. 460 p.
3. Məmmədov, C. İ. Kritik Infrastrukturlarda Informasiya Təhdidlərinin və Risklərinin Təhlili, Informasiyanın Qorunması Istiqamətlərinin Müəyyən Edilməsi / C. İ. Məmmədov, Z. M. Məmmədov, E. E. Bədəlov // Heydər Əliyev adına AAHM-in Elmi Əsərlər Məcmuəsi. 2020. No 1 (на азербайджанском языке).
4. Баутов, А. Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. СУБД. 2002. № 2. https://www.osp.ru/os/2002/02/181118/.
5. Gasimov, V. A. Construction and Realization Methods of Effective Structures of Security Service Systems in Open Computer Networks / V. A. Gasimov // Abstract of the Thesis for the Degree of Candidate of Technical Sciences. Baku, 1998. 26 p.
6. Аббасов, А. М. Проблемы информационной безопасности в компьютерных сетях / А. М. Аббасов, Р. М. Алгулиев, В. А. Касумов. Баку: Элм, 1998. 235 с.
7. Касумов, В. А. Разработка эффективной структуры системы безопасности информации для корпоративных компьютерных сетей / В. А. Касумов, С. З. Мамедов // Наукові праці Одеська національна академія зв'язку ім. О. С. Попова. 2007. № 2. С. 70–73.

References

1. Gasimov V. A., Amashov Y. A., Aliyeva F. P., Mustafayeva E. A., Mutin D. I. Bolnokin V. E. (2019) Development of the Information Security System Effective Structure for the Distributed Computer Networks. *IOP Conf. Series: Materials Science and Engineering*. 537. https://iopscience.iop.org/article/10.1088/1757-899X/537/5/052034/pdf.
2. Knapp E., Langill J. (2014) *Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid SCADA, and Other Industrial Control Systems*. Syngress Publ. 2nd ed. 460.

3. Mammadov J. I., Mammadov Z. M., Badalov E. E. (2020) Analysis of Information Threats and Risks in Critical Infrastructures, Determination of Information Protection Directions. *Collection of Scientific Works of AAHM named after Heydar Aliyev*. (1) (in Azeerb.).
4. Bautov A. (2002) An Economic View of the Problems of Information Security. *Open Systems. SMDB*. (2). https://www.osp.ru/os/2002/02/181118/ (in Russian).
5. Gasimov V. A. (1998) Construction and Realization Methods of Effective Structures of Security Service Systems in Open Computer Networks. *Abstract of the Thesis for the Degree of Candidate of Technical Sciences*. Baku. 26.
6. Abbasov A. M., Alguliev R. M., Gasimov V. A. (1998) *Problems of Information Security in Computer Networks*. Baku, Elm Publ. 235 (in Russian).
7. Gasimov V. A., Mamedov S. Z. (2007) Development of an Effective Structure of Information Security System for Corporate Computer Networks. *Scientific Works of the Odessa National Academy of Communications named after O. S. Popova*. (2), 70–73 (in Russian).

Вклад авторов / Authors' contribution

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

Сведения об авторах

Касумов В. А., д. т. н., профессор, заведующий кафедрой компьютерных технологий Азербайджанского технического университета

Мамедов Дж. И., к. т. н., доцент, доцент кафедры компьютерных технологий Азербайджанского технического университета

Адрес для корреспонденции

AZ 1073, Республика Арербайджан,
г. Баку, просп. Г. Джавида, 25
Азербайджанский технический университет
Тел.: +994 12 539-11-38
E-mail: gasumov@yahoo.com
Касумов Вагиф Алиджавад

Information about the authors

Gasimov V. A., Dr. of Sci. (Eng.), Professor, Head at the Department of Computer Technologies of the Azerbaijan Technical University

Mammadov J. I., Cand. of Sci., Associate Professor, Associate Professor at the Department of Computer Technologies of the Azerbaijan Technical University

Address for correspondence

AZ 1073, Republic of Azerbaijan,
Baku, H. Javida Ave., 25
Azerbaijan Technical University
Tel.: +994 12 539-11-38
E-mail: gasumov@yahoo.com
Gasimov Vagif Alijavad