УДК 681.322 Вестник УрФО № 3(29) / 2018, с. 43–49

**Хализев В. Н., Фёдоров С. Ю., Жданова Н. В.** DOI: 10.14529/SECUR180307

# МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИНТЕЗА ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕОРИИ ИГР И ПРИМЕНЕНИЯ КВАЛИМЕТРИЧЕСКОЙ ОЦЕНКИ КАЧЕСТВА

*Проблема оптимизации выбора при принятии решений присутствует во всех сферах жизни и деятельности современного человека. Люди принимают решения каждый день, независимо от времени и места нахождения. Многие из решений кажутся нам незначительными, а за некоторые человек, группа, целое предприятие или даже государство несет большую ответственность, в том числе и материальную. В статье рассмотрена математическая модель, позволяющая из предложенных на рынке компонентов оборудования, на основе анализа требований и сравнительного анализа, проведённого на основе квалиметрической оценки качеств выбрать оптимальное решение для синтеза интегрированной системы безопасности.*

***Ключевые слова:*** *математическая модель, синтез, анализ требований, интегрированная система безопасности.*

# *MATHEMATICAL MODEL OF SYNTHESIS OF INTEGRATED SECURITY SYSTEM BASED ON THE THEORY OF GAMES AND APPLICATION OF QUALIMETRIC QUALITY ASSESSMENT*

*The problem of optimization of choice when making decisions is present in all spheres of life and activity of a modern person. People make decisions every day, regardless of time and location. Many of the decisions seem insignificant to us, and for some people, a group, a whole enterprise or even a state bears a great responsibility, including material ones. The article discusses a mathematical model that allows the equipment components offered on the market to select the optimal solution for the synthesis of an integrated security system based on requirements analysis and comparative analysis based on a qualimetric quality assessment.*

***Keywords:*** *mathematical model, synthesis, requirements analysis, integrated security system.*

При проектировании интегрированных систем безопасности, на проектировщике лежит большая ответственность за выбор набор элементов. Принимаемое решение, очевидно, должно быть наилучшим из представленных альтернатив, однако рассмотреть все аспекты и детали, которые могут влиять на выбор в принятии решения практически невозможно. Естественно, есть исключения, и можно произвести расчеты и сравнения параметров вручную, но затраты и усилия для обработки такого количества информации будут огромными. Между тем, неоптимальность принимаемых решений ведет к значительным потерям времени, возможностей и ресурсов.

В наши дни на предприятиях и объектах в целях повышения технической оснащенности стали широко применяться интегрированные системы безопасности (ИСБ). Интегрированная система безопасности представляет собой аппаратно-программный комплекс технических средств, обладающих технической, информационной, программной и эксплуатационной совместимостью. Использование таких систем позволяет решать на новом качественном уровне задачи по обеспечению безопасности объектов, повышать эффективность действий службы безопасности.

Как правило, ИСБ включают в себя совместно функционирующие подсистемы охранной, тревожной, пожарной сигнализации и пожарной автоматики, телевизионную систему наблюдения (ТСН), системы контроля и управления доступом, систему защиты автоматизированных рабочих мест сотрудника службы безопасности, а также ряд дополнительных подсистем, обеспечивающих защиту от различных видов угроз. В состав ИСБ могут входить как изделия разных производителей, так и комплексы систем физической защиты объектов одной торговой марки. Все подсистемы, входящие в состав ИСБ имеют разнообразные количественные и качественные характеристики и параметры. К качественным характеристики можно отнести адаптируемость подсистемы под различные условия эксплуатации. Количественные параметры более разнообразны, к ним можно отнести

напряжение питания, тип и размеры зоны обнаружения, чувствительность, вероятность обнаружения, время наработки на ложное срабатывание и прочие. Так в результате анализа средств обнаружения по физическому принципу действия можно выделить множество видов и типов элементов.

Перед проектировщиком возникает проблема выбора элементов для построения ИСБ для конкретного объекта, что является трудной задачей в связи с большим количеством фирм-производителей, появившимся разнообразием систем и их комплектующих, а также индивидуальными особенностями объектов и запрашиваемого заказчиком решения. Перед специалистом возникает задача формирования такого набора средств защиты, который будет удовлетворять всем запрашиваемым условиям, требованиям и пожеланием заказчика.

В соответствии с ГОСТ Р 22.1.12, ГОСТ Р 50775 и ГОСТ Р 50776 в состав комплексной системы безопасности (КСБ) должны входить следующие технические подсистемы: 1) дежурно-диспетчерская; 2)производственно-технологического контроля; 3) охранной и тревожной сигнализации; 4) пожарной сигнализации; 5) контроля и управления доступом; 6) теле/видеонаблюдения и контроля; 7) досмотра и поиска; 8)пожарной автоматики; 9) связи с объектом; 10) защиты информации; 11)инженерно-технических средств физической защиты; 12) инженерного обеспечения объекта (электроосвещения и электропитания; газоснабжения; водоснабжения; канализации; поддержания микроклимата). [1, 2, 3]

Все эти подсистемы могут входить в состав ИСБ, но не все они обязательны при проектировании. Изучая требования заказчика и уже имеющиеся на объекте элементы КСБ, специалист по защите информации должен анализировать необходимость включения какой-либо из подсистем, а также и включения дополнительных подсистем с новыми качествами. Также необходимо учитывать пожелания заказчика при приобретении оборудования и осуществлении связанных с установкой и эксплуатацией материальных затрат. Не имеет смысла приобретать заведомо дорогостоящие компоненты ИСБ, если их стоимость превышает максимальный суммарный ущерб, наносимый объекту. Таким образом, в случае постановки задачи заказчиком, не предусматривающей проектирования конкретной подсистемы, а подразумевающей создание комплекса подсистем, входящих в состав интегрированной системы безопасности, необходимо начать проектирование с этапа выбора набора подсистем физической защиты, необходимых и достаточных для минимизации ущерба. Эта проблема находит свое решение в математическом методе изучения оптимальных стратегий, а именно теории игр.

Теория игр - это математические методы, изучающие поиск оптимальных стратегий в различных ситуациях. Для поиска наиболее оптимальной стратегии или нескольких альтернативных стратегий защиты информации можно провести математическую игру двух противоборствующих сторон, одной из которых является система защиты информации (компьютерной и (или) физической безопасности) на объекте, а другая подразумевающая возможные действия злоумышленника. Так как цель создания системы безопасности – это определение оптимальной стратегии злоумышленника и его действий, то можно считать, что преступник увлечен желанием нанести как можно больший ущерб этой разрабатываемой системе безопасности. [4]

Из предположения следует, что выигрыш нарушителя будет равен проигрышу «защитника», таким образом можно получить матрицу для антагонистической игры двух противоборствующих сторон с нулевой суммой. В качестве стратегий злоумышленника примем строки матрицы $x_i$, где $i=1,...,n$, а в качестве стратегий администратора безопасности обозначим столбцы $y_j$, где $j=1,...,m$. К стратегиям нарушителя отнесем различные виды действий, наносящих ущерб системе безопасности, а к стратегиям «защитника» отнесем применением им различных компонентов и подсистем интегрированных систем безопасности.

Для проведения игры необходимо знать результаты игры А при каждой паре стратегий $x_i$ и $y_j$. Обозначим $a_{ij}$ - причинённый преступником материальный ущерб, $p_{ij}$ - вероятность нанесения ущерба при $x_i$. В качестве $a_{ij}$ можно учитывать годовые материальные потери предприятия при реализации определенного типа угроз. Следует учитывать, что использование систем безопасности требует дополнительного финансирования (стоимость оборудования и его годового обслуживания), поэтому это тоже необходимо учесть при расчетах. Таким образом, необходимо построить такую стратегию $y_i$, при которой

сведутся к минимуму средние потери: $\sum_{i-1}^{n} a_{ij} p(x_i)$.

Для выбора оптимального набора компонентов интегрированной системы безопасности в математической игре в качестве стратегий необходимо использовать различные сочетания из угроз и методов защиты. Предположим, 1-й игрок (злоумышленник) выбирает свою стратегию *i*. В наихудшем случае он получит выигрыш min aij. Предвидя это, 1-й игрок должен выбрать свою стратегию i0 таким образом, чтобы сделать этот выигрыш лучшим:

$$\min_j a_{i_0 j} = \max_i \min_j a_{ij} \qquad (1)$$

В этом случае 2-й игрок «защитник» должен выбрать такую свою стратегию j0 чтобы получить минимальный ущерб:

$$\min_i a_{ij_0} = \min_j \max_i a_{ij} . \qquad (2)$$

Выигрыш 1-го игрока должен лежать между правыми частями формул, он называется значением игры и равен элементу $a_{i0j0}$. Действия «защитника» будут верными в том случае, если максимальный суммарный ущерб, нанесенный злоумышленником, будет сведен к минимуму.

Итак, ранее определили, что первый этап проектирования ИСБ состоит в определении входящих в систему подсистем. Для этого необходимо разложить математическую игру, где на стороне «защитника» будут различные компоненты и подсистемы, входящие в состав интегрированной системы безопасности, а на противоположной стороне – требования заказчика. В данном случае выполнение требования заказчика выражается, как «перекрывание» его определенной подсистемой и будет считаться наиболее благоприятным исходом. По итогу разложения игры выбирается комплекс, состоящий из выполняющих требования подсистем, достаточных для построения оптимальной интегрированной системы безопасности.

Следующий этап состоит в «наполнении» каждой подсистемы элементами. Для определения моделей оборудования и ПО раскладывается новая игра, в которой на стороне «защитника» уже будут элементы подсистем безопасности, а на стороне нарушителя – угрозы, возможные на исследуемом объекте, функции и требования, возложенные на подсистему.

На данном этапе возникает проблема расчета ущерба от реализации этих угроз. То есть, максимальный ущерб – это общее количество ресурсов, которые может потерять предприятие в случае реализации угроз нарушителем. Следовательно, при противодействии какой-то определенной угрозе или набору угроз с помощью компонентов и подсистем безопасности ИСБ, величина максимального ущерба будет уменьшаться. Но не стоит забывать, что практически все элементы системы, их установка и ежегодное обслуживание тоже несут потери ресурсов.

Таким образом, суммарный максимальный ущерб будет рассчитываться, как сумма максимального ущерба с учетом применения интегрированной системы безопасности и ресурсов, вложенных в эту систему. Ресурсы, вложенные в ИСБ, – это стоимость оборудования, стоимость его обслуживания (установка, ремонт, замена и т.д.), при необходимости, заработная плата персонала, рассчитанные за годовой период. Сумма максимального ущерба - это ежегодные потери из-за угроз, выраженные в денежном эквиваленте.

Далее предлагается рассчитать, во сколько раз уменьшится максимальный ущерб, в случае применения интегрированной системы безопасности. Для определения степени влияния того или иного продукта на величину максимального ущерба в расчеты можно ввести такой элемент, как «коэффициент влияния», который будет вычисляться на каждый компонент, программу или комплекс оборудования в отдельности, с помощью методов квалиметрической оценки качества продукции.

Термин «квалиметрия» впервые был предложен группой советских учёных еще в 1968 году. Азгальдов Г. Г., Гличев А. В. и другие научные работники предложили единую методику количественной оценки качества различных объектов и процессов. Квалиметрия - это наука о методах формирования количественных представлений о качестве, иными словами, это оценка качества, значимости и эффективности применения продукции. В настоящее время данная научная дисциплина широко используется при определении показателей качества для потребителей, оценке качества закупаемой продукции с целью анализа рынка, совершенствовании технологического процесса производства на основе потребительских требований, ведении количественных показателей качества объектов на основе учета перспектив научно-технического прогресса, различных требова-

ний и международных стандартов. Основная задача квалиметрии - это разработка методик оценки конкретного объекта или процесса, числом, характеризующим степень его соответствия предъявляемым требованиям. [5]

Оценивание объектов с помощью методов квалиметрии происходит поэтапно. На начальном этапе имеется определенный набор компонентов и подсистем интегрированной системы безопасности, которые имеют схожие характеристики и единую целевую направленность. Далее необходимо произвести оценку каждого элемента по различным критериям и определить число, характеризующее степень его соответствия предъявляемым требованиям и ожиданиям. После того, как произведен выбор оптимального компонента ИСБ на основе теории игр, необходимо с помощью квалиметрического расчета определить коэффициент влияния на максимальный суммарный ущерб (стоимость применения оборудования + максимальный ущерб от реализации угроз), наносимый предприятию до применения системы безопасности. Далее, используя полученные для каждого компонента коэффициенты влияния на максимальный суммарный ущерб, производится расчет, при котором определяется оптимальный набор компонентов и подсистем ИСБ, то есть максимальный суммарный ущерб при использовании которого будет сведен к минимуму. Таким образом, конечным этапом оценки продукта является принятие решения: «использовать» - «не использовать».

Так же следует отметить, что оптимальный набор средств защиты информации не является статичным, он может изменяться при изменении списка угроз и изменении показаний максимального ущерба. Данный вывод связан с тем, что стоимость оборудования будет различаться и может существенно влиять на величину полученного максимального суммарного ущерба. Эту зависимость мы можем наблюдать с помощью формул:

$$МСУ = МУ + СО \quad (3)$$

$$МСУ^* = МУ * К_в + СО \quad (4)$$

где МСУ – максимальный суммарный ущерб

МУ – максимальный ущерб

СО – стоимость оборудования

$К_в$ – коэффициент влияния

$МСУ^*$ - полученный максимальный суммарный ущерб

Любое набор компонентов и подсистем ИСБ можно охарактеризовать множеством различных показателей. Для расчета коэффициента влияния необходимо построить дерево общих свойств. Пример такого дерева представлен на рисунке 1:


Рис. 1. Начальные уровни дерева общих свойств

Для каждой функциональной группы компонентов и подсистем ИСБ строится свое индивидуальное дерево общих свойств, в котором выделяют только те свойства, которые влияют на качество обеспечения безопасности по своей функциональной направленности.

На следующем этапе проводится анализ, то есть количественная оценка качества на основе формирования определяющих показателей. Суть этого этапа состоит в определении весомостей показателей, получении необходимого количества определяющих показателей, используемых на последующих стадиях расчетов. Существуют десятки способов определения коэффициентов весомости. Один из самых популярных – это способ вспомогательной процентной шкалы. Такой способ является эффективным, так как для его реализации необходимо составить опрос экспертов по определенным критериям.

Для начала, составитель анкеты формирует дерево общих свойств для каждого ком-

понента и подсистемы ИСБ. Для одной функциональной группы компонентов, подсистем или программного обеспечения составляются одинаковые анкеты, так как смысл оптимизации состоит в выборе одного элемента из всей функциональной группы (например, к одной функциональной группе можно отнести объемные извещатели). Далее названия всех ветвей дерева, не имеющих последующего разветвления, записываются в анкету. Это критерии качества. Анкета отдается эксперту, которому необходимо определить оценки в баллах для каждого критерия качества продукта. В первой графе эксперт определяет степень важности критерия для продукта данной функциональной группы, во второй графе – оценку продукта по данному критерию. В данном случае экспертами выступают люди, непосредственно связанные с областью применения или активно применяющие оцениваемые продукты. Для точности расчета необходимо опросить как минимум 12 экспертов.

На следующем шаге складываются баллы первой графы оценивания и переводятся степень важности каждого критерия в проценты, затем в доли. Сумма степеней важности критериев в процентах равна 100%, в долях – 1, соответственно. Степень важности критерия (в долях) умножаем на оценку критерия и складываем с остальными показателями, получаем, в данном случае, суммарный коэффициент весомости Квес равный значению от 1 до 10. Чем больше коэффициент Квес, тем лучше элемент выполняет свои функциональные задачи.

Далее следует перевести $К_{вес}$ в доли и рассчитать коэффициент влияния:

$$К_{в} = 1 - К_{вес} \quad (5)$$

Формула 5 представлена таким образом потому, что коэффициент влияния, фактически, показывает во сколько раз, увеличится максимальный ущерб при применении данного продукта. Полученные коэффициенты влияния для конкретной модели устройства усредняются, так как анкетирование производится среди множества экспертов. Далее полученный результат подставляются в формулу 4 и рассчитывается величина максимального суммарного ущерба. Значения МСУ* сравниваются у всех продуктов одной функциональной группы. Выбирается компонент и подсистема интегрированной системы безопасности с наименьшим значением данного показателя. Исходя из положений теории игр, использование именно этого компонента (одного средства или подсистемы) будет наиболее оптимальным.

Также следует учитывать, что большое расхождение в баллах говорит о межэкспертной несогласованности. Сравнение производится отдельно по каждой ветви дерева. Уровень согласованности в зависимости от ответственности задачи устанавливают в размере ±5% для более ответственных задач и ±10% для менее ответственных задач. Если расхождения в оценках экспертов укладываются в этот интервал, то их считают согласованными. В случае, если оценки экспертов являются несогласованными, то их просят пересмотреть свои исходные оценки, анкетирование проводится повторно.

Таким образом, в настоящей статье предлагается решение проблем, возникающих при разработке проектов интегрированной системы безопасности. Методика позволяет на основе анализа требований, предъявляемых к обеспечению безопасности объекта, и индивидуальных предпочтений заказчика выбирать оптимальный набор оборудования и программного обеспечения для синтеза интегрированной системы безопасности из различных компонентов и подсистем, предложенных на рынке.

**Литература**


1. ГОСТ Р 22.1.12-2005 Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. - Режим доступа: http://docs.cntd.ru/document/1200039543. Дата обращения: 09.03.2018.

2. ГОСТ Р 50775 Системы тревожной сигнализации. - Режим доступа: http://www.arseng.ru/pdf/gost_r_50775-95.pdf. (Дата обращения: 09.03.2018)

3. ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) Системы тревожной сигнализации. - Режим доступа: http://docs.cntd.ru/document/1200005308. (Дата обращения: 09.03.2018)

4. Гуц А.К, Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие – Издательство Омского государственного университета, 2013. – 160 с.

5. Газарян Н.В. Квалиметрия и экспертиза качества продукции и услуг: методические указания к

практическим занятиям. КубГТУ, каф. Стандартизации, сертификации и аналитического контроля. – Краснодар, 2015. – 33 с.

**Refereces**

1. GOST R 22.1.12-2005 Bezopasnost' v chrezvychaynykh situatsiyakh. Strukturirovannaya sistema monitoringa i upravleniya inzhenernymi sistemami zdaniy i sooruzheniy. - Rezhim dostupa: http://docs.cntd.ru/document/1200039543. Data obrashcheniya: 09.03.2018.

2. GOST R 50775 Sistemy trevozhnoy signalizatsii. - Rezhim dostupa: http://www.arseng.ru/pdf/gost_r_50775-95.pdf. (Data obrashcheniya: 09.03.2018).

3. GOST R 50776-95 (MEK 60839-1-4:1989) Sistemy trevozhnoy signalizatsii. - Rezhim dostupa: http://docs.cntd.ru/document/1200005308. (Data obrashcheniya: 09.03.2018).

4. Guts A.K, Vakhniy T.V. Teoriya igr i zashchita komp'yuternykh sistem: uchebnoye posobiye – Izdatel'stvo Omskogo gosudarstvennogo universiteta, 2013. – 160 s.

5. Gazaryan N.V. Kvalimetriya i ekspertiza kachestva produktsii i uslug: metodicheskiye ukazaniya k prakticheskim zanyatiyam. KubGTU, kaf. Standartizatsii, sertifikatsii i analiticheskogo kontrolya. – Krasnodar, 2015. – 33 s.

---

**ХАЛИЗЕВ Вячеслав Николаевич,** кандидат технических наук, профессор кафедры компьютерных технологий и информационной безопасности Института компьютерных систем и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет», Россия, 350072, г. Краснодар, ул. Московская, д. 2. E-mail: ha53@mail.ru.

**ФЕДОРОВ Сергей Юрьевич,** старший преподаватель кафедры компьютерных технологий и информационной безопасности Института компьютерных систем и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет», Россия, 350072, г. Краснодар, ул. Московская, д. 2. E-mail: iitib@rambler.ru.

**ЖДАНОВА Наталья Владимировна,** студентка кафедры компьютерных технологий и информационной безопасности, Института компьютерных систем и информационной безопасности ФГБОУ ВО «Кубанский государственный технологический университет», Россия, 350072, г. Краснодар, ул. Московская, д. 2. E-mail: natalia.zhdanova.kras@mail.ru

**VYACHESLAV Nikolaevich Halizev,** Candidate of Technical Sciences, Professor of the Department of Computer Technologies and Information Security of the Institute of Computer Systems and Information Security of FSBEI HE "Kuban State Technological University", 350072, Krasnodar, st. Moskovskaya, 2. E-mail: ha53@mail.ru.

**SERGEY Yuryevich Fedorov,** Senior Lecturer, Department of Computer Technologies and Information Security, Institute of Computer Systems and Information Security, FSBEI HE "Kuban State Technological University", Russia, 350072, Krasnodar, st. Moskovskaya, 2. E-mail: iitib@rambler.ru.

**NATALYA Zhdanova,** Student, Department of Computer Technologies and Information Security, Institute of Computer Systems and Information Security, FSBEI HE "Kuban State Technological University", Russia, 350072, Krasnodar, st. Moskovskaya, 2. E-mail: natalia.zhdanova.kras@mail.ru.