ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.53

DOI: 10.21822/2073-6185-2025-52-2-169-179 Оригинальная статья /Original article

Математическая модель количественной оценки защищенности открытых операционных систем при их выборе в АС ОВД

А.И. Янгиров[1], Е.А. Рогозин[2], П.М. Дуплякин[2], Т.В. Мещерякова[2], А.О. Ефимов[2]
[1] ФКУ «НИЦ «Охрана» Росгвардии,
[1] 111539, г. Москва, Реутовская, 12Б, Россия,
[2] Воронежский институт МВД России,
[2] 394065, г. Воронеж, проспект Патриотов, 53, Россия

Резюме. Цель. В статье представлена математическая модель количественной оценки защищенности открытых операционных систем (Далее – ОС) автоматизированных систем органов внутренних дел Российской Федерации (Далее – АС ОВД РФ), разработанная на основе требований стандарта ГОСТ Р ИСО/МЭК 15408. **Метод.** Исследование проведено на основе аналитических методов: анализа возможных угроз безопасности открытых ОС и требований стандартов ГОСТ Р ИСО/МЭК 15408, анализа иерархий и применения положений нечеткой логики. **Результат.** Результатом расчета показателя защищенности анализируемой ОС является лингвистический показатель степени защищенности ОС и показатель защищенности ОС, выраженный в процентном виде. **Вывод.** Авторами предложена математическая модель количественной оценки защищенности открытых ОС при их выборе в АС ОВД РФ.

Ключевые слова: оценка защищенности, требования безопасности, банк данных угроз безопасности информации, показатель защищенности, критерии защищенности, операционная система, математическая модель

Для цитирования: А.И. Янгиров, Е.А. Рогозин, П.М. Дуплякин, Т.В. Мещерякова, А.О. Ефимов. Математическая модель количественной оценки защищенности открытых операционных систем при их выборе в АС ОВД. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(2):169-179. DOI:10.21822/2073-6185-2025-52-2-169-179

Mathematical model for quantitative assessment of the Security of open operating systems when selecting in the AS of the Internal Affairs Bodies

A.I. Yangirov[1], E.A. Rogozin[2], P.M. Duplyakin[2], T.V. Meshcheryakova[2], A.O. Efimov[2]
[1] FSI «SRC «OKHRANA» of the Federal Service of National Guard of Russia,
[1]12 B Reutovskaya St., Moscow 111539, Russia,
[2]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[2]53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. The article considers a mathematical model for quantitative assessment of the security of open operating systems (hereinafter referred to as OS) of automated systems of the internal affairs bodies of the Russian Federation (hereinafter referred to as AS OVD RF), developed based on the requirements of the standard GOST R ISO/IEC 15408. **Method.** The study was conducted based on the methods: analysis of possible threats to the security of open operating systems and the requirements of the standard GOST R ISO / IEC 15408, analysis of hierarchies and applications of fuzzy logic provisions. **Result.** The result of calculating the security indicator of the analyzed OS is a linguistic indicator of the degree of OS security and an OS security indicator expressed as a percentage. **Conclusion.** The authors propose a mathematical model for assessing the security of open operating systems when choosing them in the AS OVD RF.

Keywords: security assessment, security requirements, database of information security threats, security indicator, security criteria, operating system, mathematical model

For citation: A.I. Yangirov, E.A. Rogozin, P.M. Duplyakin,T.V. Meshcheryakova, A.O. Efimov. Mathematical model for quantitative assessment of the Security of open operating systems when selecting in the AS of the Internal Affairs Bodies. Herald of Daghestan State Technical University. Technical Sciences. 2025; 52(2):169-179. (In Russ) DOI:10.21822/2073-6185-2025-52-2-169-179.

Введение. Современная цифровая эпоха характеризуется стремительным технологическим прогрессом, который сопровождается параллельным развитием киберпреступности. Государственные структуры исполнительной власти и органы внутренних дел являются особенно уязвимыми к кибератакам.

Это обусловлено рядом факторов. Данные ведомства аккумулируют и обрабатывают огромные массивы конфиденциальной информации, представляющей высокую ценность для злоумышленников. Хищение или модификация таких данных может нанести серьезный ущерб национальной безопасности и правоохранительной деятельности.

Информационные системы государственного сектора обычно имеют более сложную и разветвленную архитектуру по сравнению с корпоративными сетями. Это значительно усложняет их защиту и создает дополнительные «точки входа» для кибератак. Наконец, высокая публичность и социальная значимость государственных органов делают их привлекательными мишенями для хакеров-активистов и других деструктивно настроенных субъектов. Успешные кибератаки на такие структуры способны вызвать широкий общественный резонанс и нанести ущерб их авторитету.

В настоящее время злоумышленники демонстрируют высокую изобретательность, постоянно совершенствуя арсенал методов и средств для взлома программно-аппаратных комплексов и получения доступа к конфиденциальным данным. Эта динамика создает существенные вызовы для специалистов в области информационной безопасности, вынуждая их уделять повышенное внимание вопросам защиты вычислительных ресурсов и критически важной информации.

Таким образом, комплексный характер стоящих перед государственными организациями задач, сложность их информационной инфраструктуры и повышенное внимание к ним со стороны злоумышленников обусловливают их уязвимость к кибератакам.

Постановка задачи. Обеспечение надежной защиты становится неотъемлемым атрибутом современной информационной инфраструктуры, требуя активизации фундаментальных и прикладных исследований, направленных на противодействие передовым методам взлома и достижение цифрового суверенитета. В этих условиях обеспечение информационной безопасности ОС АС ОВД становится одной из значимых задач, особую актуальность приобретают исследования, направленные на защиту информационных систем от несанкционированного доступа.Осо бенно атакам злоумышленников подвержены ОС АС ОВД, не предназначенные для обработки сведений, составляющих государственную тайну (Далее – открытые ОС). Такие системы зачастую функционируют в менее защищенном информационном пространстве, будучи ориентированными на решение широкого спектра прикладных задач, такие ОС обычно не обладают повышенными мерами защиты. Это делает их одной из приоритетных мишеней для устремлений киберпреступников, стремящихся получить доступ к критически важным данным и ресурсам.

В данных обстоятельствах разработка и внедрение действенных механизмов кибербезопасности открытых ОС АС ОВД, не связанных с обработкой сведений, составляющих государственную тайну, приобретает особую актуальность. Комплексный подход к обеспечению их защищенности требует интеграции передовых технологических решений, организационно-правовых мер, а также непрерывного мониторинга и реагирования на возникающие угрозы. В области защиты информационных систем от несанкционированного

доступа специалисты по безопасности применяют множество разнообразных методов, технологий и концепций. Однако для целостной оценки и принятия правильных решений по обеспечению безопасности открытых ОС необходимы обобщающие критерии, которые позволяют комплексно оценить уровень их защищенности.

В настоящее время существует большое количество частных критериев безопасности, ориентированных на отдельные аспекты ОС, например, криптостойкость алгоритмов или скорость реагирования на атаки. Но при проектировании защищенных ОС особенно важны критерии, отражающие общую защищенность системы. Такие комплексные критерии являются ключевым элементом при разработке и выборе средств защиты для АС. Они позволяют объективно оценить, насколько эффективно ОС сможет противостоять потенциальным угрозам.

Методы исследования. В Российской Федерации действует стандарт ГОСТ Р ИСО/МЭК 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», представленный в трёх частях [1,2,3]. Данные стандарты определяют систему критериев для оценки безопасности информационных технологий. При определении требований к безопасности конкретного объекта отправной точкой служит анализ его назначения и условий применения. На основе этого анализа формулируются цели безопасности, которые затем детализируются в профиле защиты или задании по безопасности. Сами требования стандарта структурированы по иерархическому принципу – от общих классов к конкретным семействам и компонентам. Каждый класс объединяет несколько семейств, а семейства, в свою очередь, содержат один или несколько отдельных компонентов.

Требования и критерии, закрепленные в данном стандарте, а также в соответствующих профилях защиты и заданиях по безопасности, могут быть использованы в качестве базиса для разработки системы показателей, применимой для оценки защищенности открытых ОС АС ОВД. Учитывая комплексный характер требований и критериев, представленных в стандарте, для практического применения наиболее целесообразным представляется их рассмотрение в рамках количественной оценки.

Количественный показатель защищенности позволит проводить оценку ОС в динамике, отслеживая их состояние в течение определенного периода времени, контролировать соблюдение требований безопасности на этапе разработки защищенных ОС, а также поспособствует оптимальному выбору ОС АС ОВД. Исследование проведено на основе аналитических методов: анализа возможных угроз безопасности открытых ОС и требований стандартов ГОСТ Р ИСО/МЭК 15408, анализа иерархий и применения положений нечеткой логики.

Обсуждение результатов. В ранее опубликованных статьях [4,5] рассматривалась общая концепция количественной оценки на основе анализа требований ГОСТ Р ИСО/МЭК 15408 (Далее – Подход) и её реализация в рамках программного обеспечения. В настоящей статье представлена математическая модель, а также отражены отдельные аспекты рассмотренного Подхода. Дальнейшим развитием представленного исследования является разработка Метода количественной оценки защищенности открытых ОС при их выборе в АС ОВД в рамках диссертационной работы, составными частями которого являются перечни угроз и критериев оценки, разработанных на основе стандартов ГОСТ Р ИСО/МЭК 15408, алгоритмы, а также математическая модель. В рассмотренном Подходе количественная оценка ОС АС ОВД производится в три этапа:

1 этап – ранжирование и выборка угроз;

2 этап – проверка соответствия требований безопасности эталонному профилю защиты, разработанного в соответствии с ГОСТ Р ИСО/МЭК 15408;

3 этап – расчет показателя защищенности анализируемой ОС.

Первый этап связан с категорированием и выборкой угроз. Характер и многообразие угроз, а также возможных факторов и последствий от их реализации затрудняют создание

единой и универсальной методологии для количественной оценки потенциального ущерба. Более того, спектр актуальных угроз постоянно расширяется в связи с технологическим прогрессом, появлением новых способов несанкционированного доступа и использованием инновационных решений, таких как искусственные нейронные сети. Учитывая внутренние нормативные требования ОВД к работе с защищенными ОС, при разработке методического подхода к количественной оценке защищенности открытых ОС целесообразно ориентироваться на существующие базы данных угроз, в которых учтены специфические требования безопасности для защищенных систем. В частности, актуальным в данном контексте является банк данных угроз безопасности информации, разработанный ФАУ «ГНИИИ ПТЗИ ФСТЭК России» [6]. Однако следует учитывать, что не все включенные в него угрозы в равной степени применимы к конкретным АС. Таким образом, при практическом использовании требуется индивидуальный выбор релевантных угроз для каждой отдельной ОС.

В указанной базе данных при реализации каждой угрозы фиксируются следующие типы возможных последствий: «нарушение конфиденциальности», «нарушение целостности» и «нарушение доступности». Характер проявления этих последствий зависит от типа реализованной угрозы. Совокупность всех учитываемых угроз в разработанном Подходе представляется множеством *T*. В рамках Подхода оценка опасности угрозы для ОС основывается на ее потенциальных последствиях. В зависимости от степени угрозы, можно выделить от одного до трех возможных исходов.

Это позволяет классифицировать угрозы в соответствии с количеством их возможных последствий. При анализе угроз безопасности можно выделить несколько категорий, базирующихся на количестве последствий реализации угрозы:

1) T_1 – угрозы, имеющие 1 возможное последствие;
2) T_2 – угрозы, имеющие 2 возможных последствия;
3) T_3 – угрозы, имеющие 3 возможных последствия.

Общее количество угроз nT, влияющих на оцениваемую ОС АС ОВД, в зависимости от количества последствий может быть представлена следующей формулой:

$$nT = \sum_{i=1}^{3} nT_i$$

$$nT = nT_1 + nT_2 + nT_3$$

где: nT_1 – общее количество угроз с 1 последствием;
nT_2 – общее количество угроз с 2 последствиями;
nT_3 – общее количество угроз с 3 последствиями.

Важно понимать, что при реализации угрозы, ее фактические последствия могут не проявиться в полной мере. Это связано с влиянием различных факторов, таких как корректность настройки системы, возникающие в процессе эксплуатации ошибки, специфические характеристики самой угрозы, актуальность используемых средств защиты и другие аспекты. Данное обстоятельства было учтено при разработке Подхода.

В рамках первого этапа Подхода предполагается, что специалист, проводящий анализ, формирует перечень возможных угроз для конкретной рассматриваемой ОС. После выборки осуществляется распределение их по степени потенциальной опасности.

На втором этапе проводится проверка соответствия реализованных в оцениваемой ОС (или ее профиле защиты) политик безопасности, целей безопасности, функциональных требований и требований доверия анализируемой ОС эталонному профилю защиты.

В статье [7] определено 6 классов защищенности профилей защиты ОС. ОС, соответствующие 1, 2 и 3 классам защиты, применяются в информационных (автоматизированных) системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, ОС, соответствующие 4, 5 и 6 классам защиты, не предназначены для обработки таких сведений. Кроме того, профили защиты 4, 5, 6 классов находятся в открытом доступе и представлены на сайте ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Помимо классификации по защищенности [7] также подразделяет ОС на 3 основных типа: тип «А», тип «Б» и тип «В». Данная типология дополняет деление ОС по классам защиты, обеспечивая более детальную характеристику ОС. В целях проведения количественной оценки защищенности ОС, используемых в АС ОВД, целесообразно применять профили защиты общего назначения (тип «А»). Такие ОС ориентированы на решение обширного количества задач и имеют расширенный функционал, что делает их более универсальными и применимыми в практике ОВД в сравнении с узкопрофильными ОС типов «Б» и «В».

С учетом отмеченного в качестве эталонного профиля защиты выбран профиль ИТ.ОС.А4.ПЗ, как наиболее защищенный вариант, применяемый для открытых ОС, и имеющий высокую практическую значимость для ОВД. Согласно рассматриваемому эталонному профилю защиты к объекту оценки предъявляются следующие требования:

– требования политик безопасности (множество *P*);
– требования предположений безопасности (множество *SA*);
– требования целей безопасности (множество *O*);
– требования целей безопасности для среды функционирования (множество *OE*);
– компоненты функциональных требований безопасности (множество *F*);
– компоненты требований доверия к безопасности (множество *R*).

В рамках Подхода множество S_{pr} включает в себя вышеуказанные множества и может быть представлена в виде:

$$S_{pr} \ni P \cup SA \cup O \cup OE \cup F \cup R$$

Анализ сложных взаимосвязей и зависимостей между представленными множествами требований, их классами, семействами и компонентами указывает на целесообразность применения метода анализа иерархий для количественной оценки таких сложноструктурированных систем. Ранее данный метод уже использовался в исследованиях для количественной оценки информационной безопасности и защищенности АС [8,9,10].

На основании представленных исследований формула для расчета количественного показателя защищенности ОС *Q* приобретает вид:

$$Q = \frac{G\left(S_{pr}, T_{\text{П}}\right)}{G\left(S_{pr}, T_{\text{М}}\right)}$$

где: $T_П$ – количество реализованных требований в оцениваемой ОС;
T_M – количество требований в эталонной ОС.

При этом количество требований в эталонной системе T_M будет всегда соответствовать общему количеству требований в множестве S_{pr}.

Количество реализованных или предъявляемых требований для множества S_{pr} приобретает вид:

$$G\left(S_{pr}, T\right) = \sum_{P_i \in P} G_i(T_P) + \sum_{SA_i \in SA} G_i(T_{SA}) + \sum_{O_i \in O} G_i(T_O) + \\ + \sum_{OE_i \in OE} G_i(T_{OE}) + \sum_{F_i \in F} G_i(T_F) + \sum_{R_i \in R} G_i(T_R)$$

где: P_i, SA_i, O_i, OE_i, F_i, R_i – отдельно выбранные требования, относящиеся к множествам *P, SA, O, OE, F, R*;

$G_i(T_P)$, $G_i(T_{SA})$, $G_i(T_O)$, $G_i(T_{OE})$, $G_i(T_F)$, $G_i(T_R)$ – степени выполнения отдельно выбранных требований.

Стоит отметить, что в эталонной системе степень выполнения требований $G_i(T_X)$ будет принимать всегда максимальное значение, равное 1.

При этом, степени выполнения требований политик безопасности, предположений безопасности, целей безопасности, целей безопасности для среды функционирования рассчитываются по упрощенной формуле, так как их направления компетенций не имеют иерархических разветвлений:

$$G_i(T_P), G_i(T_{SA}), G_i(T_O), G_i(T_{OE}) = \frac{1}{J_i}\sum_{j=1}^{J_i} C_{ij}(T_П)$$

Стандарты ГОСТ Р ИСО/МЭК 15408 вводят четкую иерархию и условия работы различных компонентов, что, в свою очередь, влияет на их весовые коэффициенты. В рамках Подхода коэффициенты распределяются равномерно, с учетом количества требований, предъявляемых к каждому компоненту. Согласно ГОСТ Р ИСО/МЭК 15408, компоненты внутри семейств функциональных требований и требований доверия имеют иерархическую зависимость. Примеры зависимостей в соответствии со стандартами представлены на рис. 1.

Рис. 1 – Примеры иерархических зависимостей компонентов
Fig. 1 – Examples of hierarchical dependency components

На рис. 1а представлена последовательная структура, где компонент с большим номером предъявляет более строгие требования, чем компонент с меньшим номером. Некоторые функциональные требования могут иметь более сложную структуру (рис. 1б).

При расчете степеней выполнения требований функциональных компонентов безопасности и компонентов доверия безопасности необходимо учесть сложные зависимости, предусмотренные ГОСТ Р ИСО/МЭК 15408. Таким образом формула для расчета $G_i(T_F)$, $G_i(T_R)$ приобретает вид:

$$G_i(T_F), G_i(T_R) = \frac{1}{J_i}\sum_{j=1}^{J_i} U_{ij}(T_П)C_{ij}(T_П)$$

$U_{ij}(T_П)$ – соответствует степени реализации требований j-го уровня. Если для данного направления компетентности нет иерархических разветвлений (зависимостей), то $U_{ij}(T_П)$ принимает значение либо 0 (требования соответствующего компонента не реализованы), либо 1. Если же есть разветвления (зависимости), то $U_{ij}(T_П)$ принимает значение относительного количества компонентов j-го уровня, требования которых выполнены. Например, $U_{i2}(T_П)$ принимает значение 1, если реализованы компоненты FAU_SAA.2 и FAU_SAA.3 и принимает значение 0,5, если реализован только один из этих компонентов (естественно при условии, что направлением компетентности является всё семейство требований FAU_SAA). При этом на третьем уровне иерархии в данном примере кроме компонента FAU_SAA.4 необходимо будет рассматривать и компонент FAU_SAA.2. Функция $C_{ij}(T_П)$ определяет коэффициент значимости используемых параметров в отдельных элементах требований.

Это значение аналогичным образом определяется как взвешенная сумма отдельных коэффициентов, характеризующих влияние тех или иных параметров. Учитываются параметры, входящие только в реализованные требования данного уровня, данного направления компетентности. Для оценки защищенности ОС, работы со сложными структурами и критериями оценки существенное значение имеет применение не только строгих технических методов, но и более гибких, ориентированных на человеческое восприятие способов с использованием удобных лингвистических формулировок. Одним из перспективных исследований в данной области является применение нечеткой логики, разработанной Лотфи Аскером Заде. Данный математический аппарат позволяет анализировать и моделировать

сложные, плохо структурируемые явления и процессы, присутствующие, в том числе, и в области обеспечения информационной безопасности. Нечеткая логика позволяет учитывать не только конкретные технические параметры, но и наличие случайных факторов и неопределенностей. Математическая модель, основанная на нечеткой логике, может достаточно точно отражать сущность моделируемых процессов, при этом адекватно работая в условиях неполноты и субъективности исходных данных. Подробное описание принципов нечеткой логики применимо к Подходу представлено в работе [11].

Многими источниками отмечается необходимость начинать обеспечение защиты от киберугроз с выявления и нейтрализации тех угроз, которые несут наиболее серьезные последствия. Например, в сборнике передового опыта [12], подготовленного Контртеррористическим управлением Организации Объединенных Наций (КТУ ООН) и Исполнительным директоратом Контртеррористического комитета Совета Безопасности Организации Объединенных Наций (ИДКТК) под председательством Интерпола в 2018 году, рассматривается мировой опыт противодействия террористическим угрозам (в том числе киберугрозам), акцентируется внимание на необходимости первоочередной концентрации усилий организаций на защите от наиболее критических угроз для достижения требуемого уровня защищенности от террористических угроз. Кроме того, согласно пункту 14.1 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации при разработке модели нарушителей и угроз в приоритете следует рассматривать наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты критической информационной инфраструктуры, с максимальными негативными последствиями [13].

Пунктом А.7.3.3 ГОСТ Р ИСО/МЭК 15408 определено, что противостояние угрозе не обязательно означает устранение угрозы, а может означать достаточное уменьшение этой угрозы или достаточное смягчение последствий реализации этой угрозы [1]. В рамках Подхода для обозначения устранения угрозы, уменьшения угрозы или смягчения последствий реализации угрозы применяется термин нивелирование угрозы.

Для функционирования нечеткой логики устанавливаются специальные правила. Правила, предусмотренные Подходом, разработаны в соответствии с ранее рассмотренным категорированием угроз в рамках 1 этапа. Правила функционирования нечеткой логики представлены на рис. 2.

Правила (условия) функционирования нечеткой логики метода количественной оценки защищенности открытых операционных систем при их выборе в АС ОВД		
Условие 1 Поскольку семейства функциональных требований, требований доверия и других критериев сложно классифицировать по уровню защиты от конкретных последствий, предполагается, что они нивелируются равномерно (отсутствие определенного требования не позволяет однозначно сказать, в каком виде выразится уязвимость ОС, так как зависимости требований могут быть многогранны)		
Условие 2 При реализации всех требований защиты эталонного профиля защиты система будет иметь максимальную защищенность		
Условие 3 Если будут нивелированы угрозы, которые имеют наибольшее количество последствий, систему можно считать однозначно минимально защищенной (множество угроз Т3)	**Условие 4** Если будут нивелированы угрозы, которые имеют 2 и 3 последствия, систему можно считать средней по уровню защищенности (множества угроз T_2 и T_3)	**Условие 5** Если будут нивелированы угрозы, имеющие 1, 2 и 3 последствия, систему можно считать максимально защищенной (множества угроз T_1, T_2 и T_3)

Рис. 2 – Правила функционирования нечеткой логики количественной оценки защищенности открытых ОС

Fig. 2 – Rules for the functioning of fuzzy logic for quantitative assessment of the security of open OS

В соответствии с установленными правилами, определим следующие степени защищенности ОС (лингвистические показатели защищенности ОС): «уязвимая система», «минимально защищенная система», «средне защищенная система», «максимально защищенная система». Исходя из изложенных выше данных, приходим к выводу, что наиболее под-

ходящим вариантом функции принадлежности для функционирования нечеткой логики будет треугольная форма. Учитывая рассмотренные ранее данные и введенные правила, сформированы функции принадлежности защищенности открытых ОС АС ОВД:

$$Q_y(N_\text{п}) = \begin{cases} 1 - \dfrac{N_\text{п}}{3nT_3}, N_\text{п} \in [0; 3nT_3); \\ 0, \text{в остальных случаях.} \end{cases}$$

$$Q_\text{мин}(N_\text{п}) = \begin{cases} 1 - \dfrac{3nT_3 - N_\text{п}}{3nT_3}, N_\text{п} \in [0; 3nT_3); \\ 1 - \dfrac{N_\text{п} - 3nT_3}{2nT_2}, N_\text{п} \in [3nT_3;\ 3nT_3 + 2nT_2); \\ 0, \text{в остальных случаях.} \end{cases}$$

$$Q_\text{ср}(N_\text{п}) = \begin{cases} 1 - \dfrac{(3nT_3 + 2nT_2) - N_\text{п}}{2nT_2}, N_\text{п} \in [3nT_3; 3nT_3 + 2nT_2); \\ 1 - \dfrac{N_\text{п} - (3nT_3 + 2nT_2)}{nT_1}, N_\text{п} \in [3nT_3 + 2nT_2; 3nT_3 + 2nT_2 + nT_1); \\ 0, \text{в остальных случаях.} \end{cases}$$

$$Q_\text{макс}(N_\text{п}) = \begin{cases} 1 - \dfrac{(3nT_3 + 2nT_2 + nT_1) - N_\text{п}}{nT_1}, N_\text{п} \in (3nT_3 + 2nT_2; 3nT_3 + 2nT_2 + nT_1]; \\ 0, \text{в остальных случаях.} \end{cases}$$

где: $Q_y(N_\text{п})$ – принадлежность к множеству «уязвимая система»;
$Q_{мин}(N_\text{п})$ – принадлежность к множеству «минимально защищенная система»;
$Q_{ср}(N_\text{п})$ – принадлежность к множеству «средне защищенная система»;
$Q_{макс}(N_\text{п})$ – принадлежность к множеству «максимально защищенная система»;
$N_\text{п}$ – количество последствий.

На основании функций принадлежности сформирован график функции соответствия диапазонов принадлежности степени защищенности открытых ОС (рис. 3).

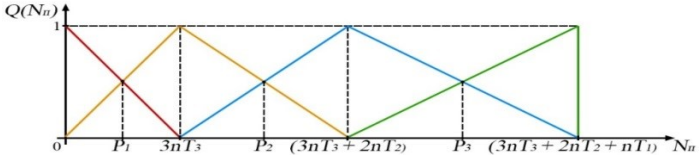

Рис. 3 – График функции соответствия диапазонов принадлежности степени защищенности открытых ОС

Fig. 3 – Graph of the function of correspondence between membership ranges of the degree of security of open OS

На рис. 3 область принадлежности к множеству «уязвимая система» обозначена красным цветом (от 0 до $3nT_3$), область принадлежности к множеству «минимально защищенная система» обозначена оранжевым цветом (от 0 до $3nT_3 + 2nT_2$), область принадлежности к множеству «средне защищенная система» обозначена синим цветом (от $3nT_3$ до $3nT_3 + 2nT_2 + nT_1$), область принадлежности к множеству «максимально защищенная система» обозначена зеленым цветом (от $3nT_3 + 2nT_2$ до $3nT_3 + 2nT_2 + nT_1$). Учитывая пересечения областей принадлежности, степени защищенности открытых ОС предполагают следующие диапазоны: «уязвимая система» – от 0 до P_1 (включительно), «минимально защищенная система» – от P_1 до P_2 (включительно), «средне защищенная система» – от P_2 до P_3 (включительно), «максимально защищенная система» – от P_3 до $3nT_3 + 2nT_2 + nT_1$ (включительно).

При рассмотрении данного способа в контексте расчета защищенности открытых ОС АС ОВД, стоит отметить, что при использовании эталонного профиля защиты предполагается, что реализация всех его требований (полная реализация на 100%) нивелирует все возможные последствия угроз (их число составляет $3nT_3 + 2nT_2 + nT_1$). В случаях реализации

в ОС меньшего количества требований пропорционально уменьшается процент защищенности ОС. Исходя из этого, выборка угроз напрямую влияет на процент защищенности системы.

Третий этап предполагает расчет показателя защищенности анализируемой ОС, а также оценивание полученного показателя защищенности ОС. На данном этапе производится вычисление соответствия политик безопасности, предположений безопасности, целей безопасности, целей безопасности для среды функционирования, функциональных требований, требований доверия к безопасности анализируемой ОС (либо профиля защиты анализируемой ОС) профилю защиты эталонной ОС, после чего производится расчет показателя защищенности анализируемой ОС по формуле:

$$Q_{\text{защ.}} = \frac{\sum P_{\text{выб.}} + \sum SA_{\text{выб.}} + \sum O_{\text{выб.}} + \sum OE_{\text{выб.}} + \sum F_{\text{выб.}} + \sum R_{\text{выб.}}}{P_{\text{эт.}} + SA_{\text{эт.}} + O_{\text{эт.}} + OE_{\text{эт.}} + F_{\text{эт.}} + R_{\text{эт.}}} \times 100\%$$

где $\sum P_{\text{выб}}$ – рассчитанное значение выбранных политик безопасности;
$\sum SA_{\text{выб}}$ – рассчитанное значение выбранных предположений безопасности;
$\sum O_{\text{выб}}$ – рассчитанное значение выбранных целей безопасности;
$\sum OE_{\text{выб}}$ – рассчитанное значение выбранных целей безопасности для среды функционирования;
$\sum F_{\text{выб}}$ – рассчитанное значение выбранных функциональных требований;
$\sum R_{\text{выб}}$ – рассчитанное значение выбранных требований доверия;
$P_{\text{эт}}$ – эталонное значение политик безопасности;
$SA_{\text{эт}}$ – эталонное значение выбранных предположений безопасности;
$O_{\text{эт}}$ – эталонное значение целей безопасности;
$OE_{\text{эт}}$ – эталонное значение выбранных целей безопасности для среды функционирования;
$F_{\text{эт}}$ – эталонное значение функциональных требований;
$R_{\text{эт}}$ – эталонное значение требований доверия.

После проведения расчета показателя защищенности анализируемой ОС производится оценивание полученного показателя в соответствии с графиком, представленным на рис. 3, и табл. 1.

Таблица 1. Определение степени защищенности ОС
Table 1. Determining the degree of OS security

Показатель защищенности ОС/OS security indicator	Степень защищенности ОС/OS security level
от 0 до P_1 (включительно)	«Уязвимая система»
от P_1 до P_2 (включительно)	«Минимально защищенная система»
от P_2 до P_3 (включительно)	«Средне защищенная система»
от P_3 до $3nT_3 + 2nT_2 + nT_1$ (включительно)	«Максимально защищенная система»

Вывод. Предложенная математическая модель является одной из составных частей Метода количественной оценки защищенности открытых ОС при их выборе в АС ОВД.

Рассмотренная в настоящем исследовании математическая модель является уникальной, не имеющей прямых аналогов на данный момент, и представляет собой новый, перспективный подход к решению задачи количественной оценки защищенности открытых ОС. Полученные в ходе реализации математической модели показатели защищенности позволяют проводить оценку ОС во временном диапазоне в динамике, осуществлять контроль требований безопасности при разработке защищенных ОС, а также осуществлять оптимальный выбор ОС для ОВД РФ.

Библиографический список:

1. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Электронный ресурс] – Режим доступа. – URL: https://docs.cntd.ru/document/1200101777 (Дата обращения: 01.08.2024).

2. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности [Электронный ресурс] – Режим доступа. – URL: https://docs.cntd.ru/document/1200105710 (Дата обращения: 01.08.2024).
3. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности [Электронный ресурс] – Режим доступа. – URL: https://docs.cntd.ru/document/1200105711 (Дата обращения: 01.08.2024).
4. Алгоритмизация расчета оценки защищенности операционных систем АИС ОВД, разработанного на основе анализа требований безопасности ГОСТ Р ИСО/МЭК 15408 и возможных угроз / А.И. Янгиров, Е.А. Рогозин, О.И. Бокова, С.Б. Ахлюстин // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 3. – С. 167-171. – DOI 10.21822/2073-6185-2023-50-3-167-171. – EDN QIOPOE.
5. Разработка автоматизированной системы расчета оценки защищенности операционных систем информационных систем на основе анализа требований безопасности / А.И. Янгиров, Е.А. Рогозин, Е.Ю. Никулина, А.В. Калач // Вестник Воронежского института ФСИН России. – 2022. – № 4. – С. 182-188. – EDN BNBXNZ.
6. Банк данных угроз безопасности информации – [Электронный ресурс] – Режим доступа. – URL: https://bdu.fstec.ru/ (Дата обращения: 04.08.2024).
7. Информационное сообщение от 18 октября 2016 г. № 240/24/4893 «Об утверждении Требований безопасности информации к операционным системам» ФСТЭК России – [Электронный ресурс] – Режим доступа. – URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-18-oktyabrya-2016-g-n-240-24-4893 (Дата обращения: 20.07.2024).
8. Способ вычисления количественного показателя защищённости автоматизированных систем на основе требований ГОСТ Р ИСО/МЭК15408-1-2013/И.Г. Дровникова, А.А. Никитин, А.А. Змеев//Вестник ВИ МВД России. 2015. №3. URL: https://cyberleninka.ru/article/n/sposob-vychisleniya-kolichestvennogo-pokazatelya-zaschischyonnostiavtomatizirovannyh-sistem-na-osnove-trebovaniy-gost-r-iso-mek-15408 (Дата обращения: 04.08.2024).
9. Разработка системы исследования информационной безопасности организации на основе метода анализа иерархии / Е.А. Арефьева, М.А. Сафронова, А.В. Никитина // Известия ТулГУ. Технические науки. 2016. №11-1. URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-issledovaniya-informatsionnoy-bezopasnosti-organizatsii-na-osnove-metoda-analiza-ierarhii (Дата обращения: 04.08.2024).
10. Использование «Общих критериев» для построения систем автоматизированного проектирования комплексов средств защиты информации/ М.А. Багаев, М.В. Коротков, Е.А. Рогозин // Вопросы защиты информации: науч. практич. журнал. – М.: ФГУП «ВИМИ», 2003. Вып. 4 (63). – С. 57.
11. К вопросу проведения количественной оценки защищенности открытых операционных систем АС ОВД РФ на основе теории нечеткой логики /А.И. Янгиров, И.М. Янгиров, Е.А. Рогозин, С.Б. Ахлюстин // Охрана, безопасность, связь. – 2024. – № 9-1. – С. 163-170. – EDN FKQAIL.
12. Защита критически важных объектов инфраструктуры от террористических атак:сборник передового опыта.URL:https://www.un.org/securitycouncil/ctc/sites/www.un.org. (дата обращения 10.08.2024).
13. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

References:

1. GOST R ISO/IEC 15408-1-2012. Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model – [Electronic resource] – Access mode. – URL: https://docs.cntd.ru/document/1200101777 (Date of access: 01.08.2024).
2. GOST R ISO/IEC 15408-2-2013. Information technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components – [Electronic resource] – Access mode. – URL: https://docs.cntd.ru/document/1200105710 (Date of access: 01.08.2024).
3. GOST R ISO/IEC 15408-3-2013. Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements – [Electronic resource] – Access mode. – URL: https://docs.cntd.ru/document/1200105711 (Date of access: 01.08.2024).
4. Algorithmization for calculating the security assessment of ais operating systems of internal affairs bodies, developed on the basis of an analysis of security requirements GOST R ISO/IEC 15408 and possible threats. A.I. Yangirov, E.A. Rogozin, O.I. Bokova, S.B. Ahlyustin. *Herald of Daghestan State Technical University. Technical Science.* 2023; 50(3):167-171. – DOI 10.21822/2073-6185-2023-50-3-167-171. – EDN QIOPOE.

5. Development of an automated system for calculating the security assessment of operating systems of information systems based on the analysis of security requirements. A.I. Yangirov, E.A. Rogozin, E.Yu. Nikulina, A.V. Kalach. *Herald of Voronezh Institute of the Russian Federal Penitentiary Service*. 2022;4: 182-188. – EDN BNBXNZ.
6. Databank of information security threats – [Electronic resource] – Access mode. – URL: https://bdu.fstec.ru/ (Date of access: 04.08.2024).
7. Information message dated October 18, 2016 № 240/24/4893 «On approval of Information Security Requirements for operating systems» FSTEC of Russia – [Electronic resource] –Access mode. – URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-18-oktyabrya-2016-g-n-240-24-4893 (Date of access:20.07.2024).
8. The method of calculating the quantitative indicator of security of the automated systems on the basis of GOST R 15408-1-2013 / Drovnikova I.G., Nikitin A.A., Zmeev A.A. // Herald of Voronezh Institute of the Ministry of Internal Affairs of Russia. 2015. №3. URL: https://cyberleninka.ru/article/n/sposob-vychisleniya-kolichestvennogo-pokazatelya-zaschischyonnosti- avtomatizirovannyh-sistem-na-osnove-trebovaniy-gost-r-iso-mek-15408 (Date of access: 04.08.2024).
9. Development of information security research organization on the basis of method of analysis hierarchy / E.A. Arefeva, M.A. Safronova, A.V. Nikitina // Tula State University News. Technical sciences. 2016. №11-1. URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-issledovaniya-informatsionnoy-bezopasnosti-organizatsii-na-osnove-metoda-analiza-ierarhii (Date of access: 04.08.2024).
10. Using «General Criteria» for Building Automated Design Systems for Information Security Systems / M.A. Bagaev, M.V. Korotkov, E.A. Rogozin.*Voprosyi zaschityi informatsii: nauch.-praktich. zhurnal*. M.: FGUP «VIMI», 2003; 4 (63):5–7.
11. On the issue of quantitative assessment of the security of open operating systems AS ATS of the Russian Federation based on the theory of fuzzy logic / A.I. Yangirov, I.M. Yangirov, E.A. Rogozin, S.B. Ahlyustin. *Security, safety, communications*. 2024;9(1):163-170. – EDN FKQAIL.
12. Protecting Critical Infrastructure from Terrorist Attacks: A Compendium of Best Practices URL: URL:https://www.un.org/securitycouncil/ctc/sites/www.un.org. (Date of access: 10.08.2024).
13. Rules for the categorization of critical information infrastructure objects of the Russian Federation, approved by Decree of the Government of the Russian Federation dated February 8, 2018 № 127 «On approval of the Rules for the categorization of critical information infrastructure objects of the Russian Federation, as well as a list of indicators of criteria for the significance of critical information infrastructure objects of the Russian Federation and their meanings».(In Russ)

Сведения об авторах:

Адиль Илдарович Янгиров, начальник отделения лабораторных исследований и испытаний; adil-yan@yandex.ru

Евгений Алексеевич Рогозин, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем ОВД; evgenirogozin@yandex.ru

Петр Михайлович Дуплякин, преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга; 00008540@mail.ru

Татьяна Вячеславовна Мещерякова, доктор технических наук, начальник кафедры автоматизированных информационных систем ОВД; mescher73@mail.ru

Алексей Олегович Ефимов, преподаватель кафедры автоматизированных информационных систем органов ОВД; ea.aleksei@yandex.ru

Information about authors:

Adil I. Yangirov, Head of the Laboratory Research and Testing; adil-yan@yandex.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Assoc. Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Pyotr M. Duplyakin, Lecturer, Department of Radio Engineering Systems and Security Monitoring Complexes; 00008540@mail.ru

Tatyana V. Meshcheryakova, Dr. Sci. (Eng.), Head of the Department of Automated Information Systems of Internal Affairs Bodies; mescher73@mail.ru

Aleksey O. Efimov, Lecturer, Department of Automated Information Systems of Internal Affairs Bodies; ea.aleksei@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 20.12.2024**.**

Одобрена после рецензирования / Reviced 29.01.2025.

Принята в печать /Accepted for publication 12.05.2025.