

17. Kalyaev I.A., Gayduk A.R., Kapustyan S.G. Modeli i algoritmy kollektivnogo upravleniya v gruppakh robotov [Models and algorithms of collective control in groups of robots]. Moscow: Fizmatlit, 2009, 278 p.
18. Bertsekas D., Castanon D. Parallel synchronous and asynchronous implementations of the auction algorithm, *Intern. J. of Parallel Computing*, 1991, Vol. 17, pp. 707-732.
19. Bruff D. The Assignment Problem and the Hungarian Method. Retrieved June 26, 2016.
20. Beloglazov D.A., Solov'ev V.V., Titov A.E. [i dr.]. Metod raspredeleniya tseley v gruppakh intellektual'nykh mobil'nykh robotov [The method of distribution of goals in groups of intelligent mobile robots], *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki* [Bulletin of the Tula State University. Technical science], 2016, No. 11-3, pp. 122-133.
21. Jukna S. Extremal Combinatorics: With Applications in Computer Science. Berlin. Springer, 2001, 375 p.

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Курейчик.

**Соловьев Виктор Владимирович** – Южный федеральный университет; e-mail: vvsolovev@sfnu.ru; г. Таганрог, Россия; тел.: +79043438844; кафедра систем автоматического управления; старший преподаватель; руководитель Центра проектной деятельности ИРТСУ ЮФУ.

**Номерчук Александр Яковлевич** – e-mail: aynomerchuk@sfnu.ru; тел. +79185945894; кафедра систем автоматического управления; старший преподаватель.

**Soloviev Viktor Vladimirovich** – Southern Federal University; e-mail: vvsolovev@sfnu.ru; Taganrog, Russia; phone: +79043438844; the department of automatic control systems; senior lecturer; head of the Center for Project Activities, Institute of Radio Engineering Systems and Control, SFU.

**Nomerchuk Alexandr Yakovlevich** – e-mail: aynomerchuk@sfnu.ru; phone: +79185945894; the department of automatic control systems; senior lecturer.

УДК 004.056.5

DOI 10.18522/2311-3103-2023-3-157-172

**С.С. Велигодский, Н.Г. Милославская**

### **УНИФИЦИРОВАННАЯ МОДЕЛЬ ЗРЕЛОСТИ ЦЕНТРОВ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ**

*Создаваемые согласно Указу Президента Российской Федерации № 250 субъектами критической информационной инфраструктуры специальные структурные подразделения способны противодействовать компьютерным атакам на их информационно-телекоммуникационные сети (ИТКС). Чтобы быть эффективными, в составе этих подразделения должны существовать центры управления сетевой безопасностью (ЦУСБ) ИТКС, имеющие высокий уровень зрелости, соответствующий предъявляемым к его организации–владельцу требованиями по обеспечению информационной безопасности. В настоящее время единого подхода к проведению оценки уровня зрелости ЦУСБ не существует. Поэтому целью статьи является описание разработанной унифицированной модели зрелости ЦУСБ ИТКС организаций (УМЗ ЦУСБ), созданной на основе обобщения и развития проанализированных моделей зрелости и собственной систематики процессов управления сетевой безопасностью (УСБ) и услуг по УСБ типовой ИТКС, реализуемыми в ЦУСБ, а также технологий, поддерживающих выполнение процессов и предоставление услуг, дополненным рассмотрением общей организации функционирования ЦУСБ и его кадровым обеспечением. Модель зрелости ЦУСБ определена как структурированный набор элементов, объединяющий информационную потребность установления уровня зрелости ЦУСБ с их атрибутами – свойствами или характеристиками ЦУСБ. Сформулированы требования к разрабатываемой УМЗ внут-*

ренного ЦУСБ организации, выполнение которых продемонстрировано в конце статьи. Введено формализованное представление модели зрелости ЦУСБ как объекта оценки уровня зрелости по пяти направлениям оценки, а именно, организационное обеспечение функционирования ЦУСБ, процессы УСБ ИТКС и ЦУСБ как ее составной части, услуги по УСБ ИТКС, предоставляемые ЦУСБ, используемые для этого технологии и кадровое обеспечение. Предложен способ наглядного отображения полученных результатов оценки в виде круговых диаграмм. Представлен подход к установлению итогового уровня зрелости ЦУСБ. Показано, что все сформулированные требования к модели зрелости ЦУСБ в разработанной УМЗ ЦУСБ ИТКС выполнены. Далее для УМЗ ЦУСБ ИТКС должна быть создана методика ее применения.

Унифицированная модель зрелости; центр управления сетевой безопасностью; информационно-телекоммуникационная сеть; направления оценки.

**S.S. Veligodskiy, N.G. Miloslavskaya**

### **UNIFIED MODEL OF MATURITY OF NETWORK SECURITY CENTERS OF INFORMATION AND TELECOMMUNICATION NETWORKS**

*In accordance with Decree No. 250 of the President of the Russian Federation, special structural units created by subjects of critical information infrastructure are able to counteract computer attacks on their information and telecommunication networks (ITCNs). In order to be effective, these units must have Network Security Centers (NSCs) of ITCN with a high level of maturity that meets the information security requirements for its owner organization. Currently, there is no single approach to assessing the NSC maturity level. Thus the article's goal is to describe the developed Unified Maturity Model (UMM) of ITCN NSCs of organizations, created based on the generalization and development of the analyzed maturity models and authors' systematics of network security management (NSM) processes and services of a typical ITCN implemented in the NSC, as well as technologies that support the implementation of processes and the provision of services, supplemented by consideration of the general organization of the NSC functioning and its staffing. The NSC maturity model refers to a structured set of elements that combines the information need to establish the NSC maturity level with their attributes – NSC properties or characteristics. The requirements for UMM being developed for the organization's internal NSC are formulated, and their implementation is demonstrated at the end of the article. A formalized representation of the maturity model of NSC as an object for assessing the maturity level in five assessment areas, namely, the organizational support for the NSC functioning, the NSM processes for ITCN and the NSC as its integral part, the ITCN NSM services provided by the NSC, the technologies used and staffing, is introduced. A method for visualizing the obtained assessment results as pie charts is proposed. An approach to establishing the final NSC maturity level is presented. It is shown that all the formulated requirements for the NSC maturity model are met in the developed ITCN NSC UMM. Further, a methodology for the ITCN NSC UMM application should be created.*

*Unified maturity model; network security center; information and telecommunications network; assessment areas.*

**Введение.** Создаваемые согласно Указу Президента Российской Федерации № 250 [1] субъектами критической информационной инфраструктуры (КИИ) специальные структурные подразделения способны противодействовать компьютерным атакам (КА) на их информационно-телекоммуникационные сети (ИТКС). Чтобы быть эффективными, в составе этих подразделения должны существовать центры управления сетевой безопасностью (ЦУСБ) ИТКС, имеющие высокий уровень зрелости, соответствующий предъявляемым к его организации–владельцу требованиями по обеспечению информационной безопасности (ИБ). В настоящее время единого подхода к проведению оценки уровня зрелости таких ЦУСБ не существует, но он необходим для определения возможных путей совершенствования ЦУСБ и для соответствующих уполномоченных органов, проводящих такую оценку.

Целью статьи является описание разработанной унифицированной модели зрелости ЦУСБ ИТКС организаций (УМЗ ЦУСБ), созданной на основе обобщения и развития проанализированных моделей зрелости и собственной систематики процессов управления сетевой безопасностью (УСБ) и услуг по УСБ типовой ИТКС, реализуемыми в ЦУСБ, а также технологий, поддерживающих выполнение процессов и предоставление услуг, дополненных рассмотрением общей организации функционирования ЦУСБ и его кадровым обеспечением.

**1. Требования к унифицированной модели зрелости ЦУСБ ИТКС.** Учитывая опыт построения моделей зрелости ЦУСБ [2–15], сформулируем требования (*Тр*) к разрабатываемой УМЗ внутреннего ЦУСБ ИТКС организации:

*Тр1:* модель должна обеспечивать достоверность (объективность), повторяемость (воспроизводимость) и сопоставимость получаемых результатов проведения оценок уровня зрелости ЦУСБ, а также последовательность проведения этих оценок и полезность их результатов для дальнейшего совершенствования ЦУСБ;

*Тр2:* в модели должна отражаться информация об УСБ ИТКС организации в целом и управлении рисками и инцидентами ИБ в ИТКС в частности как системообразующих элементах УСБ и важной обратной связи для совершенствования ОИБ ИТКС и ЦУСБ;

*Тр3:* в модели должна содержаться информация об этапах жизненного цикла ЦУСБ как структурного подразделения организации, начиная с создания и внедрения и заканчивая активным использованием и совершенствованием;

*Тр4:* модель должна базироваться на универсальном наборе четко сформулированных показателей достижения определенного уровня зрелости ЦУСБ с формализованным выставлением значений, которые они могут принимать;

*Тр5:* в модели необходимо связать показатели по пяти НО из области оценки уровня зрелости ЦУСБ и ввести для всех направлений и ЦУСБ в целом единые уровни зрелости;

*Тр6:* модель должна определять функции (методы), объединяющие полученные значения различных показателей в рамках одного НО и совместно по всем пяти НО в показатель итогового уровня зрелости ЦУСБ;

*Тр7:* главенствующую роль в определении итогового уровня зрелости ЦУСБ в модели должны играть уровни зрелости для процессов УСБ ИТКС и предоставляемых услуг по УСБ ИТКС при обязательном учете таких уровней для применяемых в ЦУСБ технологий, организационного и кадрового обеспечения;

*Тр8:* модель должна определять методы оценки всех подлежащих оценке атрибутов объектов оценки, приоритетными из которых по возможности должны быть количественные или полуколичественные (по сравнению с качественными) методы оценки;

*Тр9:* модель должна определять конкретные, достаточно простые и понятные критерии оценки каждого из атрибутов, основанные на фактах и документированной информации (конкретных свидетельствах оценки);

*Тр10:* понятия разной степени абстракции, описывающие достаточно широкий отвлеченный класс проблем или какой-либо редкий частный случай, не должны располагаться на одном уровне рассмотрения;

*Тр11:* в модели должно быть предусмотрено одновременное наличие в организации элементов ЦУСБ разных уровней зрелости и однозначность определения в такой ситуации обобщенного показателя уровня зрелости по НО, где находится такой элемент;

*Тр12:* в модели определяется уровень зрелости объектов оценки на предмет их результативности как степени реализации и достижения запланированных результатов и будущего потенциала по УСБ ИТКС (в противовес эффективности как экономической категории, учитывающей затраты на достижение запланированного результата);

*Тр13:* модель должна учитывать особенности современного развития ИТКС и технологий и средств УСБ и ОИБ, которые могут быть использованы в ЦУСБ;

*Тр14:* модель должна предоставлять эталонную шкалу уровней зрелости «развивающегося» ЦУСБ и показывать конкретные этапы развития ЦУСБ и пути перехода от одного уровня его зрелости к следующему;

*Тр15:* для модели должна быть разработана методика применения, дающая общие рекомендации по сбору исходных данных для проведения оценки зрелости ЦУСБ и упрощающая использование модели оценщиками различной квалификации, а также ее адаптацию к потребностям организации, проводящей первичную и последующие оценки уровня зрелости ЦУСБ.

**2. Формализованное представление УМЗ ЦУСБ ИТКС.** Введем определенную модель зрелости ЦУСБ ИТКС как структурированного набора элементов, объединяющего информационную потребность установления уровня зрелости ЦУСБ с их атрибутами – свойствами или характеристиками ЦУСБ (адаптировано на основе [16, 17]). Проблема обоснованного выбора атрибутов очень важна: если их слишком много, то оценка существенно затруднена из-за большого объема информации, а оценка по неправильно выбранным атрибутам приведет к неверным результатам и излишним затратам. Информационная потребность – знания (сведения), необходимые для управления целями, задачами, рисками и проблемами ЦУСБ. Потребителями информации могут выступать различные заинтересованные стороны: внутренние (собственники и органы управления, органы контроля, сервисные подразделения и т.п.) и внешние (органы надзора и регулирования, акционеры, инвесторы и т.п.) по отношению к организации, имеющей ЦУСБ.

Для описания ЦУСБ как объекта оценки уровня зрелости введем сокращенные обозначения обеспечивающих функционирование ЦУСБ направлений, определяющую область оценки:

- ◆ организационное обеспечение ЦУСБ – ОФ;
- ◆ процессы УСБ ИТКС и ЦУСБ как ее составной части, а также управления самим ЦУСБ и его деятельностью – ПУСБ;
- ◆ услуги по УСБ ИТКС ожидаемого качества, поддерживающие требуемый уровень ИБ ИТКС в соответствии со всеми применимыми требованиями по ОИБ – УУСБ;
- ◆ используемые для этого технологии – Т;
- ◆ кадровое обеспечение – К.

Тогда  $УМЗ_{ЦУСБ}$  представляется следующим кортежем, содержащим в себе пять кортежей для пяти направлений оценки уровня зрелости ЦУСБ:

$$УМЗ_{ЦУСБ} = \{ЦУСБ, \{ОФ, АФ, ШАФ, МФ, КОАФ, ФФ, ШУЗФ, УЗФ\}, (1) \\ \{ОП, АП, ШАП, МП, КОАП, ФП, ШУЗП, УЗП\}, \\ \{ОУ, АУ, ШАУ, МУ, КОАУ, ФУ, ШУЗУ, УЗУ\}, \\ \{ОТ, АТ, ШАТ, МТ, КОАТ, ФТ, ШУЗТ, УЗТ\}, \\ \{ОК, АК, ШАК, МК, КОАК, ФК, ШУЗК, УЗК\}, Ф_{ЦУСБ}, ШУЗ_{ЦУСБ}, ИУЗ_{ЦУСБ}\},$$

где  $ЦУСБ, ОФ, ОП, ОУ, ОТ, ОК$  – множество объектов оценки для ЦУСБ в целом и отдельно по каждому НО –  $ОФ = \{оф_1, оф_2, \dots, оф_L\}$ , определяющие содержание оценки уровня зрелости, причем  $L$  может быть различным для НО –  $ОФ$  (для краткости  $L_1$ ),  $ОП$  ( $L_2$ ),  $ОУ$  ( $L_3$ ),  $ОТ$  ( $L_4$ ) и  $ОК$  ( $L_5$ ). Эти объекты оценки в каждом НО могут содержать групповые объекты оценки –  $gоо$ , в которые, в свою очередь, могут входить частные объекты оценки –  $гоо$ .

$A_{Оф}, A_{ПУСБ}, A_{УУСБ}, A_T, A_K$  – множество атрибутов объектов оценки в НО, подлежащих оценке –  $A = \{a_1, a_2, \dots, a_N\}$ , причем  $N$  может быть различным для пяти НО –  $N_{Оф}$  (для краткости  $N_1$ ),  $N_{ПУСБ}$  ( $N_2$ ),  $N_{УУСБ}$  ( $N_3$ ),  $N_T$  ( $N_4$ ) и  $N_K$  ( $N_5$ );

$ША_{Оф}, ША_{ПУСБ}, ША_{УУСБ}, ША_T, ША_K$  – эталонные шкалы для НО как упорядоченные совокупности эталонных значений, которые могут принимать атрибуты объектов оценки данного НО –  $SA = \{sa_1, sa_2, \dots, sa_N\}$ ;

$M_{Оф}, M_{ПУСБ}, M_{УУСБ}, M_T, M_K$  – множество методов оценки атрибутов объектов оценки для НО –  $M = \{m_1, m_2, \dots, m_M\}$ , причем в общем случае  $M$  может различаться для пяти НО –  $M_{Оф}, M_{ПУСБ}, M_{УУСБ}, M_T$  и  $M_K$  и может быть больше (для оценки одного и того же атрибута применимы несколько альтернативных методов оценки), меньше (к некоторым атрибутам применяются одинаковые методы оценки) или равно (для каждого атрибута применяется свой уникальный метод оценки) соответствующего  $N$  ( $N_1, N_2, N_3, N_4$  или  $N_5$ );

$КОА_{Оф}, КОА_{ПУСБ}, КОА_{УУСБ}, КОА_T, КОА_K$  – критерии оценки значений атрибутов объектов оценки для НО –  $KOA = \{koa_1, koa_2, \dots, koa_N\}$ , причем в общем случае  $N$  может быть различным для пяти НО –  $N_1, N_2, N_3, N_4$  и  $N_5$ ;

$\Phi_{Оф}, \Phi_{ПУСБ}, \Phi_{УУСБ}, \Phi_T, \Phi_K$  – функции или методы, объединяющие полученные результаты оценки для всех атрибутов объектов оценки каждого НО в общий показатель уровня зрелости данного НО или числовое значение оценки, характеризующее уровень его зрелости (далее для краткости – показатель уровня зрелости);

$ШУЗ_{Оф}, ШУЗ_{ПУСБ}, ШУЗ_{УУСБ}, ШУЗ_T, ШУЗ_K$  – эталонные шкалы уровней зрелости НО;

$УЗ_{Оф}, УЗ_{ПУСБ}, УЗ_{УУСБ}, УЗ_T, УЗ_K$  – результаты оценки для НО в виде конкретного уровня зрелости оцениваемого НО;

$\Phi_{ЦУСБ}$  – функция или метод, обобщающая полученные значения уровней зрелости НО в показатель итогового уровня зрелости ЦУСБ;

$ШУЗ_{ЦУСБ}$  – эталонная шкала уровней зрелости ЦУСБ;

$ИУЗ_{ЦУСБ}$  – итоговый результат в виде конкретного уровня зрелости оцениваемого ЦУСБ.

УМЗ ЦУСБ отражает, как выбранные для каждого направления оценки атрибуты объектов оценки могут быть оценены и преобразованы в результаты оценки, служащие основой для принятия решений об уровне зрелости данного направления (рис. 1) (на основе [17]). Отметим, что процесс получения итогового интегрального уровня зрелости ЦУСБ здесь не отражен.

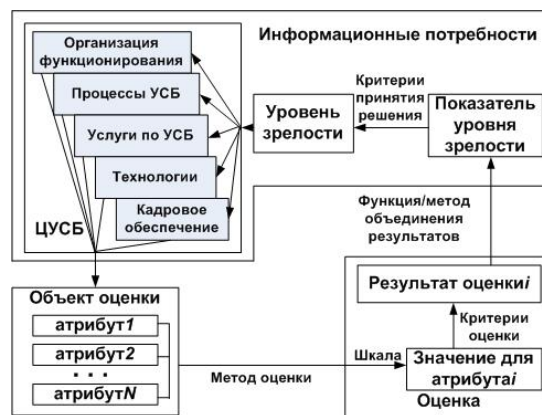


Рис. 1. Оценивание объектов оценки ЦУСБ по пяти направлениям согласно УМЗ ЦУСБ ИТКС

Объекты оценки со своими специфическими атрибутами устанавливаются для каждого направления оценки и представляют собой отдельные реализованные процессы УСБ ИТКС, предоставляемые услуги по УСБ ИТКС, используемые при этом технологии и прочее. Каждый объект оценки можно детализировать, введя более мелкие – частные – объекты оценки, назвав его тогда групповым объектом оценки.

В ходе оценки для каждого атрибута объекта оценки на основе применения соответствующего метода оценки определяются их количественные значения как результаты некоторого расчета или измерения и (или) качественные характеристики как результаты анализа или наблюдения. Оценка представляет собой суждение об этих результатах. Метод оценки – логическая последовательность операций, прямо или косвенно определяющая, как количественно или качественно оценивать атрибуты каждого объекта оценки посредством применения принятой эталонной шкалы. Эталонная шкала определяет для каждого атрибута целевые значения (или их диапазоны (интервалы) и пороговые значения) или их характеристики, соответствующие установленным уровням зрелости. Критерии оценки значений для атрибутов содержат совокупности требований, характеризующих определенный уровень их зрелости. Результатом оценки является обобщенная характеристика атрибутов объекта оценки, дающую качественную или количественную оценку степени его зрелости на основе ее сравнения с критериями оценки в рамках определенной шкалы эталонных значений и интерпретация полученной характеристики, понятная потребителю оценки. Качество результата оценки зависит в первую очередь от исходных данных, на основе которых производилась оценка.

Для УМЗ ЦУСБ принципиальным является выполнение условия, при котором ни один из объектов оценки из определенного ниже базового набора для каждого направления оценки не может быть исключен (не выбран) или оставлен не оцененным (в отличие от подходов Банка России [18] и ГОСТ Р 57580.2-2018 [19]). Для каждого объекта оценки должен быть установлен уровень его зрелости, обязательно учитываемый при оценке обобщенного уровня зрелости всего направления оценки. В противном случае определить уровень зрелости направления оценки, в который попадает данный объект, не представляется возможным, а, значит, нельзя и установить уровень зрелости всего ЦУСБ.

В случае существенного отклонения полученного значения атрибута от целевого значения необходимо выявить причины отклонения и предложить меры по усовершенствованию объекта оценки, устранившие их.

При проведении последующих оценок результат оценки покажет динамическое изменение значения для атрибута за определенный период времени после первой оценки, т.е. повысился уровень его зрелости, упал или остался на прежнем уровне.

Критерии оценки значений для атрибутов должны быть просты и понятны и сформулированы, например, исходя из критичности атрибута для объекта оценки в рамках его вклада в выполнение основного назначения данного направления оценки в УСБ ИТКС или ЦУСБ в целом, текущего уровня зрелости атрибута, уровня зрелости атрибутов связанных с данным объектом оценки и т.п. Критерии могут быть, например, следующего вида [20]:

♦ счетные, например, «Количество процессов от их общего числа, обладающие определенным свойством» или «Процент процессов от их общего числа, обладающих определенным свойством» (сравнение с данным критерием относит полученный результат к одному из диапазонов возможных значений, которые может принимать атрибут) или сумма инвестиций в проекты ЦУСБ и затраты на ОИБ;

- ◆ основанные на наблюдаемых фактах, например, «Все посетители помещений ЦУСБ регистрируются системой видеонаблюдения» (форма ответа при сравнении с данным критерием – «Да» или «Нет»);
- ◆ основанные на анкетах, содержащих формулировки счетных и основанных на наблюдаемых фактах критериев и поля для внесения результатов;
- ◆ в виде каких-либо требований, например, наличие лицензии на осуществление какой-либо деятельности.

Использование сразу нескольких критериев для одного объекта оценки дает возможность повысить точность оценки.

В качестве единой эталонной шкалы для каждого выбранного атрибута в УМЗ ЦУСБ установим следующую шкалу от «0» до «1» с равным шагом как доли от максимального значения или характеристики атрибута:

- ◆ «неудовлетворительно» (не достигается/не существует или крайне мало свидетельств достижения/существования, неявный, незафиксированный письменно) – в диапазоне 0-0,19(9),
- ◆ «мало» (в основном или в значительной степени не достигается/не существует, некоторые аспекты достижения атрибута непредсказуемы; явный, зафиксированный письменно, но неформализованный каким-либо образом) – в диапазоне 0,2-0,39(9),
- ◆ «удовлетворительно» (частично достигается/существует, явный, формализованный, заверенный и опубликованный) – в диапазоне 0,4-0,59(9),
- ◆ «хорошо» (в основном или в значительной степени с редкими исключениями достигается/существует, существуют некоторые недостатки достигаемых значений атрибутов; явный, проверенный и подлежащий контролю) – в диапазоне 0,6-0,79(9) и
- ◆ «отлично» (полностью или всегда достигается/существует; значительных недостатков, связанных с полученным значением атрибута, не выявлено) – в диапазоне 0,8-1.

После накопления опыта применения УМЗ ЦУСБ на практике значения границ интервалов могут быть в дальнейшем пересмотрены, что не отразится на самом процессе оценки уровня зрелости ЦУСБ, а только на конечном результате этой оценки. Отметим, что все значения границ интервалов могут быть умножены на 100%, если при проведении оценки такой подход более понятен и нагляден для отображения ее результатов.

Фактические обобщенные (объединенные) значения частных атрибутов сначала в групповые для одного объекта оценки, а далее для всех объектов оценки одного направления – в показатель уровня зрелости этого направления. После применения критериев принятия решения он имеет вид уровня зрелости для конкретного направления оценки и демонстрирует конкретные характеристики этого направления, соответствующие установленному уровню зрелости.

Значение  $z a_{lpji}$  для каждого  $i$ -го атрибута  $j$ -го частного объекта оценки  $p$ -го группового объекта оценки  $l$ -го объекта оценки в рамках одного НО из общего числа  $L$  ( $L_1, L_2, L_3, L_4$  или  $L_5$  соответственно) рассчитывается как среднее арифметическое значение субъективной оценки  $z a_{lpji}$  всех  $Q$  опрошиваемых лиц (их порядковые номера обозначены индексом  $q$ ), мнение которых имеет равную значимость (в общем случае  $Q$  для разных атрибутов различны), по принятой шкале по формуле:

$$\bar{z a}_{lpj} = \frac{\sum_{q=1}^Q z a_{lpjiq}}{Q} \quad (2)$$

В эту формулу можно ввести весовые коэффициенты, учитывающие степень компетентности опрашиваемых лиц, что усложнит дальнейшие расчеты и саму процедуру оценки, поскольку придется дополнительно определять эту компетентность, увеличивая временные и трудовые затраты на общую оценку уровня зрелости. В частном (вырожденном) случае, когда для получения значения атрибута можно опросить только одно лицо, среднее значение и будет равно значению, которое выставило это лицо.

Показатель уровня зрелости по каждому атрибуту одного частного объекта оценки оценивают путем сопоставления значений атрибутов со значениями эталонными шкалы. Поскольку эталонная шкала устанавливает значения для атрибутов  $z a_{l p j i}$  в диапазоне от «0» до «1», как и для весовых коэффициентов, то в итоге обобщенное значение для всех атрибутов одного группового объекта оценки также будет принимать значение от «0» до «1» (за счет того, что сумма всех весовых коэффициентов равна «1»). [При использовании значений в процентах обобщенное значение также будет находиться в диапазоне от «0» до «100».]

Сумма взвешенных значений показателей уровня зрелости  $z o o_l$  всех  $L$  ( $L_1, L_2, L_3, L_4$  или  $L_5$  соответственно) объектов оценки в рамках одного НО позволяет рассчитать показатель уровня зрелости ПУЗ этого НО (вторая строка кратко и первая строка развернуто):

$$\begin{aligned}
 \text{ПУЗ} = & \sum_{i=1}^L w o o_l * \left( \sum_{p=1}^P w g o o_{l p} * \left( \sum_{j=1}^J w r o o_{l p j} * \left( \sum_{i=1}^N w a_{l p j i} * z a_{l p j i} \right) \right) \right) = \quad (3) \\
 & \sum_{i=1}^L w o o_l * z o o_l \quad \sum_{p=1}^P w g o o_{l p} * z g o o_{l p} \quad \sum_{j=1}^J w r o o_{l p j} * z r o o_{l p j} \quad \sum_{i=1}^N w a_{l p j i} * z a_{l p j i}
 \end{aligned}$$

Сумма взвешенных значений показателей уровня зрелости  $z g o o_{l p}$  всех  $P$  групповых объектов оценки позволяет рассчитать показатель уровня зрелости  $z o o_l$  объекта оценки в рамках НО (третья строка кратко).

Сумма взвешенных значений показателей уровня зрелости  $z r o o_{l p j}$  всех  $J$  частных объектов оценки позволяет рассчитать показатель уровня зрелости  $z g o o_{l p}$  группового объекта оценки (четвертая строка формулы кратко).

Сумма взвешенных значений всех  $N$  ( $N_1, N_2, N_3, N_4$  или  $N_5$  соответственно) атрибутов  $a_{l p j i}$  частных объектов оценки  $r o o_{l p j}$  позволяет рассчитать показатель уровня зрелости  $z r o o_{l p j}$  этого частного объекта оценки (пятая строка).

При этом суммы весовых коэффициентов  $w o o_l, w g o o_{l p}, w r o o_{l p j}$  и  $w a_{l p j i}$  вклада соответствующего значения или показателя в общий показатель для всех видов весовых коэффициентов равны «1». Установление таких коэффициентов проводится один раз, например, путем опроса экспертов или на основе собранной статистики. Возможные значения весовых коэффициентов обсуждаются в последующих разделах, посвященных отдельным НО.

Для получение показателя уровня зрелости каждого НО в баллах полученное значение ПУЗ в диапазоне от «0» до «1» умножается на 100.

В формулу (3) можно было бы дополнительно ввести корректирующий коэффициент неравномерности, уравнивающий полученные групповые значения в случае их большого разброса, когда в одной группе они очень высокие, а в другой



– очень низкие. Но при оценке уровня зрелости это представляется нелогичным, ибо основная задача оценки – выявить реальную картину, а не усредненную («сглаженную»).

Также для каждого из результатов оценки и обобщенного показателя уровня зрелости ЦУСБ могут быть определены желательные тенденции их изменения при росте уровня зрелости. Таким образом, в УМЗ ЦУСБ заложен итерационный процесс совершенствования ЦУСБ на основе повышения результатов систематически проводимой оценки уровня зрелости ЦУСБ.

Критерии принятия решения необходимы для определения конкретного уровня зрелости по соответствию ему показателя уровня зрелости ЦУСБ.

Важно отметить, что количество уровней зрелости для всех пяти направлений оценки для удобства дальнейшей интеграции в единый итоговый уровень зрелости ЦУСБ логично установить одинаковым. Обобщив результаты проведенного анализа моделей уровней зрелости для различных объектов оценки и исключив нулевой уровень (отсутствие объекта оценки), с целью обеспечения наибольшей преемственности с имеющимися моделями зрелости в УМЗ ЦУСБ представляется обоснованным определить пять уровней зрелости направлений оценки и самого ЦУСБ в целом с едиными названиями – *«начальный»*, *«базовый и повторяемый»*, *«установившийся и отслеживаемый»*, *«управляемый и измеряемый»*, *«оптимизируемый и устойчивый»* соответственно. Для перехода от первого уровня ко второму добавляется анализ и повторяемость, от второго к третьему – стандартизация и отслеживаемость, от третьего к четвертому – управляемость и измеряемость и от четвертого к пятому – устойчивость, оптимизируемость и постоянное совершенствование.

Продолжая ранее представленные рассуждения, общая оценка уровня зрелости ЦУСБ или отдельного направления оценки может составлять от 0 до 100 баллов. Предлагаются следующие уровни зрелости, связанные с определенным количеством набранных в процессе оценки баллов (при этом важно, что за количеством баллов стоит соответствующий перечень характеристик для каждого уровня):

- ◆ *«начальный»* – в диапазоне 0-19,99(9) баллов, когда деятельность иерархически организованного ЦУСБ по УСБ ИТКС осуществляется хаотически, от случая к случаю, без единого подхода (так называемое «ситуационное управление» (*Ad hoc*)); сами процессы УСБ непредсказуемы и слабо контролируемы.

- ◆ *«базовый и повторяемый»* – в диапазоне 20-39,99(9) баллов, когда одинаковые задачи по УСБ ИТКС решаются разными людьми схожими методами, но формализованные процедуры УСБ и распределение ответственности отсутствуют, что увеличивает вероятность ошибок; часто процессы УСБ появляются в ответ на определенные события, а затраты на них могут превышать выделенный бюджет;

- ◆ *«установившийся и отслеживаемый»* – в диапазоне 40-59,99(9) баллов, когда процедуры УСБ определены на уровне ЦУСБ (он может быть представлен как некий «конвейер по УСБ ИТКС»), стандартизованы (формализуют существующую практику) и документированы, исполняются заблаговременно с управлением качеством, но возможно с превышением бюджета и не всегда прослеживаемыми отклонениями;

- ◆ *«управляемый и измеряемый»* – в диапазоне 60-79,99(9) баллов, когда ЦУСБ контролирует по целям и измеряет процессы УСБ по показателям и принимает меры, если они нерезультативны и неэффективны (но риск этого в тактической перспективе минимален, хотя и возможен в стратегической перспективе); могут использоваться инструменты их автоматизации;

- ◆ *«оптимизируемый и устойчивый»* – в диапазоне 80-100 баллов, когда процессы УСБ ИТКС, реализуемые ЦУСБ с сетевой организационной структурой, развиты в рамках заранее определяемого бюджета до уровня хорошей практики

(риски в тактической и стратегической перспективах минимальны) в результате постоянных улучшений и сравнений, т.е. осуществляется управление изменениями, инновациями и знаниями.

Как и в случае с границами значений интервалов для оценки атрибутов объектов оценки, после накопления опыта применения УМЗ ЦУСБ на практике значения границ интервалов для уровней зрелости ЦУСБ могут быть в дальнейшем пересмотрены, что не отразится на самом процессе оценки уровня зрелости ЦУСБ, а только на конечном результате этой оценки.

В качестве метода, объединяющего полученные значения уровней зрелости направлений оценки в единый показатель уровня зрелости ЦУСБ, логично выбрать минимальное значение из показателей для всех пяти направлений (согласно давно известному в ИБ принципу – «уровень ИБ всей системы не может быть выше уровня ИБ самого слабого ее звена»), а не их интегральное значение по какой-либо формуле. Кроме того нельзя говорить о некоем математическом равенстве уровней зрелости всех пяти направлений оценки, но все они важны для достижения высокого уровня зрелости ЦУСБ.

**3. Итоговый уровень зрелости ЦУСБ ИТКС.** По аналогии с подходом Банка России [18], рис. 2 содержит три круговые диаграммы: первая и третья отображают обобщенные результаты оценки уровней зрелости направлений ОФ и К соответственно, а на второй одновременно отображаются результаты оценки уровней зрелости направлений ПУСБ, УУСБ и Т, поскольку групповые объекты оценки направлений УУСБ и Т жестко связаны с таковыми для групповых объектов оценки направления ПУСБ.

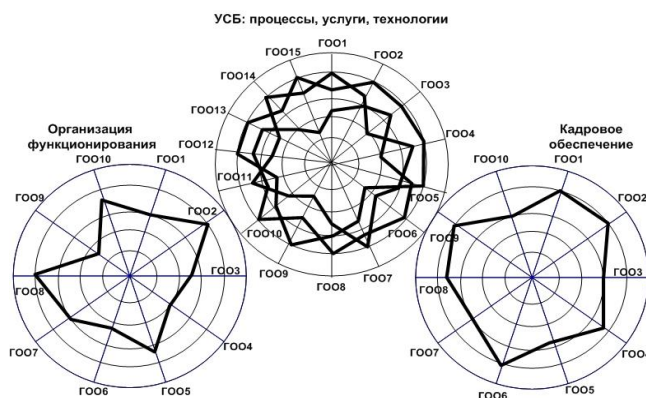


Рис. 2. Вид круговых диаграмм для отображения показателей уровней зрелости направлений оценки ЦУСБ

Значения показателей уровня зрелости каждого основного группового объекта оценки направлений ПУСБ, УУСБ и Т отображаются на верхней круговой диаграмме на прямых, разделяющих сектора с 1-го по 12-й, а каждого вспомогательного – на прямых, разделяющих сектора с 12-го по 1-ый, точкой, отстающей от центра круговой диаграммы на величину, соответствующую значениям этих показателей. Шаг перехода с одного уровня зрелости на другой равен «0,2», что показано на каждой из трех диаграмм четырьмя равноотстоящими внутренними окружностями.

Значения показателей уровня зрелости каждого основного группового объекта оценки направлений ОФ и К отображаются соответственно на левой и правой круговых диаграммах на прямых, разделяющих сектора с 1-го по 10-й, точкой, отстающей от центра круговой диаграммы на величину, соответствующую значениям этих показателей.

Пятому уровню зрелости всех объектов оценки пяти направлений соответствует окружность радиусом 0,8 и кольцо до окружности радиусом «1», четвертому – окружность радиусом 0,6 и кольцо до окружности радиусом 0,8, третьему – окружность радиусом 0,4 и кольцо до окружности радиусом 0,6, второму – окружность радиусом 0,2 и кольцо до окружности радиусом 0,4 и первому – круг до окружности радиусом 0,2.

Значение итогового уровня зрелости ЦУСБ  $IUZ_{ЦУСБ}$  логично определять по наименьшему значению из пяти уровней зрелости по пяти направлениям оценки, пересчитанные в баллы (умноженные на 100) и имеющие значения от 0 до 100 баллов (пример представлен на рис. 3):

$$IUZ_{ЦУСБ} = \min(UZ_{ОФ}, UZ_{ПУСБ}, UZ_{УУСБ}, UZ_T, UZ_K), \quad (4)$$

где  $UZ_{ОФ}$  – уровень зрелости направления ОФ;  
 $UZ_{ПУСБ}$  – уровень зрелости направления ПУСБ;  
 $UZ_{УУСБ}$  – уровень зрелости направления УУСБ;  
 $UZ_T$  – уровень зрелости направления Т;  
 $UZ_K$  – уровень зрелости направления К.

Направления оценки	Уровни зрелости				
	1-ый	2-ой	3-ий	4-ый	5-ый
ОФ			45		
ПУСБ			56		
УУСБ				65	
Т				63	
К			47		
ЦУСБ			45		

Рис. 3. Примеры значений уровней зрелости направлений оценки ЦУСБ и ЦУСБ в целом

По количеству полученных баллов определяется уровень зрелости ЦУСБ как «начальный», если минимальное значение попадает в диапазон 0-19,99(9) баллов; «базовый и повторяемый» – в диапазон 20-39,99(9) баллов; «установившийся и отслеживаемый» – в диапазон 40-59,99(9) баллов; «управляемый и измеряемый» – в диапазон 60-79,99(9) баллов или «оптимизируемый и устойчивый» – в диапазон 80-100 баллов.

#### 4. Выполнение сформулированных требований к УМЗ ЦУСБ ИТКС.

Обобщая полученные в исследовании результаты, покажем, что все ранее сформулированные требования к УМЗ ЦУСБ ИТКС выполнены (табл. 1).

Таблица 1

#### Выполнение сформулированных требований к УМЗ ЦУСБ ИТКС

Требование	Комментарий по выполнению требования
Тр1	Достоверность подтверждается использованием российских ГОСТов и международных стандартов, а повторяемость и сопоставимость обеспечиваются точностью и правильностью свидетельств оценки, а также единой методикой оценки уровня зрелости ЦУСБ с применением УМЗ при систематически повторяющемся процессе оценки уровня зрелости ЦУСБ.
Тр2	Процессы УСБ ИТКС положены в основу УМЗ, среди которых важнейшее место занимают детально описанные процессы управления рисками и инцидентами ИБ.

Окончание табл. 1

Tr3	Такая информация учтена и оценивается при оценке уровня зрелости НО ОФ.
Tr4	В УМЗ установлены единые для всех направлений и объектов оценки показатели уровня зрелости.
Tr5	Показатели уровней зрелости трех направлений – ПУСБ, УУСБ и Т жестко связаны между собой и их уровень зрелости опирается на уровень зрелости ОФ и К.
Tr6	Разработанные формулы (2)-(4) для расчетов демонстрируют установление таких функций.
Tr7	Атрибуты оценки объектов в рамках направлений УУСБ и Т сформулированы с учетом атрибутов НО ПУСБ. Количество этих атрибутов больше, чем для направлений ОФ и К. Роль показателей каждого НО при установлении итогового уровня зрелости ЦУСБ учтена в формуле (4).
Tr8	В исследовании указаны возможные методы оценки с применением эталонной шкалы, определяющей для каждого атрибута пороговые значения и их характеристики, соответствующие установленным уровням зрелости. Для каждого НО для выбранного в качестве примера объекта оценки приведены смысловые значения введенной эталонной шкалы.
Tr9	В исследовании показано как формулируются критерии оценки атрибутов объектов оценки. Для выбранного в качестве примера объекта оценки приведены смысловые значения критериев оценки.
Tr10	Определены объекты оценки, для которых выделяются «подобъекты» второго (групповые) и третьего (частные) уровней иерархии (например, «подпроцессы» и «подподпроцессы»).
Tr11	Выставление оценщиками существенно различающихся значений для атрибутов одного объекта оценки сглаживается за счет вычисления среднего арифметического этих значений (формула (2)). УМЗ допускает для разных объектов оценки большой разброс значений, поскольку важно выявить реальную картину, а не усредненную («сглаженную»).
Tr12	Понятие «эффективность» упоминается только при оценке уровня зрелости НО ОФ ЦУСБ.
Tr13	В исследовании упоминаются все известные на текущий момент технологии ОИБ и СЗИ, но при этом для всех групповых объектов оценки список частных объектов не закрыт (поставлены троеточия, означающие возможность расширения приведенных перечней).
Tr14	Эталонная шкала уровней зрелости ЦУСБ приведена в разделе 2. Пути перехода от одного уровня зрелости к другому связаны с усовершенствованием конкретных объектов оценки, для которых при предыдущей оценке был определен более низкий уровень зрелости.
Tr15	Разработанная методика оценка уровня зрелости ЦУСБ с применением УМЗ ЦУСБ описана в исследовании отдельно.

Таким образом, на основе проведенного анализа можно сделать вывод, что все сформулированные требования к УМЗ ЦУСБ ИТКС удовлетворены.

Можно выделить следующие достоинства разработанной УМЗ ЦУСБ ИТКС:

- ◆ строится на основе комплексного подхода к описанию системы управления инцидентами ИБ для ИТКС в организации на основе внедрения и использования ЦУСБ;

- ◆ содержит понятную систему описания элементов ЦУСБ в виде иерархии взаимосвязанных элементов (лучшие практики, используемые технологии и средства, реализуемые процессы и их функциональность, кадровое обеспечение, результаты и показатели);

- ◆ позволяет оценить на основе установленных критериев уровень зрелости процессов управления инцидентами ИБ в ЦУСБ, причем как для всего процесса в целом, так и по отдельности для каждого его подпроцесса, выступая индикатором

сильных и слабых сторон их реализации и использования, позволяя анализировать связанные с процессами рисков в отношении их определенной качественной характеристики и в связи с определенным контекстом их использования, «подсвечивая» те области, которые за текущими задачами остаются не замеченными;

- ◆ позволяет оценить эффективность ЦУСБ как инфраструктуры, которая поддерживает требуемый уровень ИБ ИТКС организации;

- ◆ позволяет оценить требуемый уровень управления инцидентами ИБ на основе внедрения ЦУСБ, необходимый для достижения основных целей ведения бизнеса организации;

- ◆ задает направление для дальнейшего развития ЦУСБ организации в области управления инцидентами ИБ и позволяет сформулировать ключевые действия, которые необходимо выполнить для продвижения на следующий уровень модели зрелости.

**Заключение.** Учитывая опыт и лучшие практики оценки зрелости различных объектов, а также недостатки известных моделей зрелости, сформулированы требования к разрабатываемой УМЗ собственного ЦУСБ организации в целом и ее отдельным элементам, выполнение которых показано в последнем разделе.

Для описания ЦУСБ как объекта оценки уровня зрелости с пятью направлениями оценки введена модель уровня зрелости ЦУСБ  $УМЗ_{ЦУСБ}$ , которая представлена в виде кортежа, содержащего в себе пять кортежей для пяти направлений оценки (формула 1). Элементами  $УМЗ_{ЦУСБ}$  являются множество объектов оценки в целом (ЦУСБ) и отдельно по каждому направлению оценки, множество атрибутов более мелких объектов оценки в рамках каждого направления, эталонные шкалы значений, которые могут принимать атрибуты объектов оценки данного направления, множество методов оценки этих атрибутов и критерии оценки значений атрибутов, функции (методы), объединяющие полученные результаты оценки для всех атрибутов объектов оценки каждого направления в единый показатель уровня зрелости данного направления, эталонные шкалы уровней зрелости для каждого направления, результаты оценки каждого направления в виде конкретного уровня зрелости, функция (метод), обобщающая полученные значения уровней зрелости направлений в единый показатель уровня зрелости ЦУСБ, эталонная шкала уровней зрелости ЦУСБ и итоговый результат оценки в виде конкретного уровня зрелости оцениваемого ЦУСБ.

Предложен способ визуализации оценки уровней зрелости направлений оценки ЦУСБ по групповым объектам оценки в рамках каждого направления в виде трех круговых диаграмм (по одной для направлений оценки ОФ и К и одной обобщенной для взаимосвязанных направлений оценки ПУСБ, УУСБ и Т) для принятия решения об итоговом уровне зрелости ЦУСБ и последующих действий по повышению зрелости конкретных объектов оценки.

Отличительной чертой разработанной УМЗ ЦУСБ ИТКС является ее универсальность, позволяющая применять ее при оценке ЦУСБ разного уровня зрелости с типовым набором объектов оценки по пяти направления и используемую в организациях различного размера, области деятельности и подчиненности. Эта модель может быть адаптирована под потребности конкретной организации (например, в части уточнения объектов оценки и их атрибутов), которая начинает построение своего ЦУСБ. По мере роста и «созревания» операционных потребностей организации ЦУСБ также будет адаптироваться и развиваться.

Далее для разработанной УМЗ ЦУСБ ИТКС создается методика ее применения.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
2. *Gardiner M.* The Critical Incident Response Maturity Journey. – EMC Corporation, 2013. – Режим доступа: [http://docs.media.bitpipe.com/io\\_11x/io\\_115661/item\\_894499/Critical%20Incident%20Response%20Maturity.pdf](http://docs.media.bitpipe.com/io_11x/io_115661/item_894499/Critical%20Incident%20Response%20Maturity.pdf) (дата обращения: 29.05.2023).
3. SIM3: Security Incident Management Maturity Model. – Open CSIRT Foundation, 2019. – Режим доступа: <http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf> (дата обращения: 29.05.2023).
4. CSIRT capabilities: How to assess maturity? Guidelines for national and governmental CSIRTs. – ENISA, 2016. – Режим доступа: <https://www.enisa.europa.eu/publications/csirt-capabilities> (дата обращения: 29.05.2023).
5. *Dorofee A., Ruefle R., Zajicek M., McIntire D., Alberts C., Perl S., Huth C.L., Walters P.* Incident Management Capability Assessment. – Software Engineering Institute of Carnegie Mellon University, 2018. – Режим доступа: [https://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2018\\_005\\_001\\_538866.pdf](https://resources.sei.cmu.edu/asset_files/TechnicalReport/2018_005_001_538866.pdf) (дата обращения: 29.05.2023).
6. *Wahlgren G.A.* Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents. Academic dissertation for the Degree of Doctor of Philosophy in Computer and Systems Sciences. – Stockholm University, 2020. – Режим доступа: <https://www.diva-portal.org/smash/get/diva2:1411275/FULLTEXT01.pdf> (дата обращения: 29.05.2023).
7. State of security operations. – Hewlett-Packard, 2014. – Режим доступа: <http://h41382.www4.hp.com/gfs-shared/downloads-303.pdf> (дата обращения: 29.05.2023).
8. Os V.R. SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers. Master Thesis, Information Security Program. – Luleå University of Technology, 2016. – 75 p.
9. SOC-CMM Introduction. – SOC-CMM, 2020. – Режим доступа: <https://www.soc-cmm.com/introduction> (дата обращения: 29.05.2023).
10. Nettitude Blog: Cybersecurity Maturity Assessments Explained. – Nettitude, 2020. – Режим доступа: <https://blog.nettitude.com/cyber-maturity-assessments-explained-nettitude> (дата обращения: 29.05.2023).
11. Three Levels of SOC Maturity: Steps for Continual Service Improvement. – Huntsman, 2018. – Режим доступа: <https://www.huntsmansecurity.com/blog/three-levels-of-soc-maturity-steps-for-continual-service-improvement/> (дата обращения: 29.05.2023).
12. *Kuzbari T.* Security Operations Center. Part 2 – Internal SOC maturity levels. – Cybereason, 2018. – Режим доступа: <https://www.linkedin.com/pulse/security-operations-center-part-2-internal-soc-maturity-kuzbari> (дата обращения: 29.05.2023).
13. *Crump J.* Security Operations Center – Use Case Maturity Model/Cube (SOC-UCMM). – 2018. – Режим доступа: <https://www.jeffreydoncrump.com/post/security-operations-centre-soc-managed-security-service-provider-monitoring-content-maturity-cube> (дата обращения: 29.05.2023).
14. Построение и развитие центров мониторинга информационной безопасности (SOC). – PwC, 2019. – Режим доступа: <https://www.pwc.ru/ru/services/technology/cyber-security/soc.html> (дата обращения: 29.05.2023).
15. The Security Operations Maturity Model: A Practical Guide to Assessing and Improving the Capabilities of Your Security Operations Center. – LogRhythm, 2019. – Режим доступа: <https://logrhythm.com/security-operations-maturity-model-white-paper/> (дата обращения: 29.05.2023).
16. ISO/IEC/IEEE 15939:2017 Systems and software engineering – Measurement process. – 2017. – 39 p.
17. ГОСТ Р ИСО/МЭК 27004–2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. – Введ. 2021-11-30. – М.: Стандартинформ, 2021. – 46 с.
18. Стандарт Банка России СТО БР ИББС-1.2-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014. – Введ.: 2014-06-01. – М., 2014. – 101 с.

19. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. – Введ. 2018-03-28. – М.: Стандартинформ, 2018. – 23 с.
20. *Репин В.* Оценка зрелости системы управления бизнес-процессами компании. – 2020. – Режим доступа: [https://www.businessstudio.ru/articles/article/otsenka\\_zrelosti\\_sistemy\\_upravleniya\\_biznes\\_protseessami\\_repin/](https://www.businessstudio.ru/articles/article/otsenka_zrelosti_sistemy_upravleniya_biznes_protseessami_repin/) (дата обращения: 29.05.2023).

#### REFERENCES

1. Ukaz Prezidenta Rossiyskoy Federatsii ot 1 maya 2022 g. № 250 «O dopolnitel'nykh merakh po obespecheniyu informatsionnoy bezopasnosti Rossiyskoy Federatsii» [Decree of the President of the Russian Federation of May 1, 2022 No. 250 “On Additional Measures to Ensure the Information Security of the Russian Federation”].
2. *Gardiner M.* The Critical Incident Response Maturity Journey. EMC Corporation, 2013. Available at: [http://docs.media.bitpipe.com/io\\_11x/io\\_115661/item\\_894499/Critical%20Incident%20Response%20Maturity.pdf](http://docs.media.bitpipe.com/io_11x/io_115661/item_894499/Critical%20Incident%20Response%20Maturity.pdf) (accessed 29 May 2023).
3. SIM3: Security Incident Management Maturity Model. Open CSIRT Foundation, 2019. Available at: <http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf> (accessed 29 May 2023).
4. CSIRT capabilities: How to assess maturity? Guidelines for national and governmental CSIRTs. ENISA, 2016. Available at: <https://www.enisa.europa.eu/publications/csirt-capabilities> (accessed 29 May 2023).
5. *Dorofee A., Ruefle R., Zajicek M., McIntire D., Alberts C., Perl S., Huth C.L., Walters P.* Incident Management Capability Assessment. Software Engineering Institute of Carnegie Mellon University, 2018. Available at: [https://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2018\\_005\\_001\\_538866.pdf](https://resources.sei.cmu.edu/asset_files/TechnicalReport/2018_005_001_538866.pdf) (accessed 29 May 2023).
6. *Wahlgren G.A.* Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents. Academic dissertation for the Degree of Doctor of Philosophy in Computer and Systems Sciences. Stockholm University, 2020. Available at: <https://www.diva-portal.org/smash/get/diva2:1411275/FULLTEXT01.pdf> (accessed 29 May 2023).
7. State of security operations. Hewlett-Packard, 2014. Available at: <http://h41382.www4.hp.com/gfs-shared/downloads-303.pdf> (accessed 29 May 2023).
8. Os V.R. SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers. Master Thesis, Information Security Program. Luleå University of Technology, 2016, 75 p.
9. SOC-CMM Introduction. SOC-CMM, 2020. Available at: <https://www.soc-cmm.com/introduction> (accessed 29 May 2023).
10. Nettitude Blog: Cybersecurity Maturity Assessments Explained. Nettitude, 2020. Available at: <https://blog.nettitude.com/cyber-maturity-assessments-explained-nettitude> (accessed 29 May 2023).
11. Three Levels of SOC Maturity: Steps for Continual Service Improvement. Huntsman, 2018. Available at: <https://www.huntsmansecurity.com/blog/three-levels-of-soc-maturity-steps-for-continual-service-improvement/> (accessed 29 May 2023).
12. *Kuzbari T.* Security Operations Center. Part 2 – Internal SOC maturity levels. Cybereason, 2018. Available at: <https://www.linkedin.com/pulse/security-operations-center-part-2-internal-soc-maturity-kuzbari> (accessed 29 May 2023).
13. *Crump J.* Security Operations Center – Use Case Maturity Model/Cube (SOC-UCMM), 2018. Available at: <https://www.jeffreydoncrump.com/post/security-operations-centre-soc-managed-security-service-provider-monitoring-content-maturity-cube> (accessed 29 May 2023).
14. Postroenie i razvitie tsentrov monitoringa informatsionnoy bezopasnosti (SOC) [Construction and development of information security monitoring centers (SOC)]. PwC, 2019. Available at: <https://www.pwc.ru/ru/services/technology/cyber-security/soc.html> (accessed 29 May 2023).
15. The Security Operations Maturity Model: A Practical Guide to Assessing and Improving the Capabilities of Your Security Operations Center. LogRhythm, 2019. Available at: <https://logrhythm.com/security-operations-maturity-model-white-paper/> (accessed 29 May 2023).
16. ISO/IEC/IEEE 15939:2017 Systems and software engineering – Measurement process, 2017, 39 p.
17. GOST R ISO/MEK 27004–2021 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment informatsionnoy bezopasnosti. Monitoring, otsenka zashchishchennosti, analiz i otsenivanie [GOST R ISO/IEC 27004–2021 Information technology. Security techniques. Information security management. Monitoring, security assessment, analysis and evaluation]. Introd. 2021-11-30. Moscow: Standartinform, 2021, 46 p.

18. Standart Banka Rossii STO BR IBBS-1.2-2014 Obespechenie informatsionnoy bezopasnosti organizatsiy bankovskoy sistemy Rossiyskoy Federatsii. Metodika otsenki sootvetstviya informatsionnoy bezopasnosti organizatsiy bankovskoy sistemy Rossiyskoy Federatsii trebovaniyam STO BR IBBS-1.0-2014 [Standard of the Bank of Russia STO BR IBBS-1.2-2014 Ensuring information security of organizations of the banking system of the Russian Federation. Methodology for assessing the compliance of information security of organizations of the banking system of the Russian Federation with the requirements of STO BR IBBS-1.0-2014]. Introd.: 2014-06-01. Moscow, 2014, 101 p.
19. GOST R 57580.2-2018 Bezopasnost' finansovykh (bankovskikh) operatsiy. Zashchita informatsii finansovykh organizatsiy. Metodika otsenki sootvetstviya [GOST R 57580.2-2018 Security of financial (banking) transactions. Protection of information of financial organizations. Conformity assessment methodology]. Introd. 2018-03-28. Moscow: Standartinform, 2018, 23 p.
20. *Repin V. Otsenka zrelosti sistemy upravleniya biznes-protsessami kompanii* [Evaluation of the maturity of the company's business process management system], 2020. Available at: [https://www.businessstudio.ru/articles/article/otsenka\\_zrelosti\\_sistemy\\_upravleniya\\_biznes\\_pr\\_otsessami\\_repin/](https://www.businessstudio.ru/articles/article/otsenka_zrelosti_sistemy_upravleniya_biznes_pr_otsessami_repin/) (accessed 29 May 2023).

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Курейчик.

**Велигодский Сергей Сергеевич** – Национальный исследовательский ядерный университет «МИФИ»; e-mail: SSVelagodsky@sberbank.ru; г. Москва, Россия; тел.: 89263868400; инженер.

**Милославская Наталья Георгиевна** – e-mail: NGMiloslavskaya@mephi.ru; тел.: 89166776599; д.т.н.; доцент; профессор.

**Veligodskiy Sergey Sergeevich** – National Research Nuclear University MEPHI; e-mail: SSVelagodsky@sberbank.ru; Moscow, Russia; phone: +79263868400; engineer.

**Miloslavskaya Natalia Georgievna** – e-mail: NGMiloslavskaya@mephi.ru; phone: +79166776599; dr. of eng. sc.; associate professor; professor.

УДК 621.3.078:519.713

DOI 10.18522/2311-3103-2023-3-172-188

**В.В. Соловьев, А.Я. Номерчук**

## **АВТОМАТНАЯ МОДЕЛЬ КРУИЗ-КОНТРОЛЯ ДЛЯ АВТОМОБИЛЯ**

*Целью данной работы является разработка автоматной модели круиз-контроля автомобиля, модели его прямолинейного движения и их комплексного исследования. Данная работа является актуальной в связи с отсутствием систем адаптивного круиз-контроля на отечественных автомобилях, высокой загруженности магистралей и утомительному для водителя движению в пробках. Для достижения поставленной цели в работе решена задача разработки автоматной модели системы круиз-контроля, включающей десять возможных состояний с учетом взаимодействия с штатными подсистемами автомобиля и радаром. В модели учтены диапазоны изменения скоростей движения автомобиля в зависимости от оборотов двигателя, а также оценивается длительность торможения в зависимости от дорожной обстановки и состояния подсистем автомобиля. На основе автоматной модели получены шесть сценариев работы системы круиз-контроля, учитывающие возможные ошибки и управляющие воздействия на подсистемы автомобиля в зависимости от текущей ситуации. При разработке модели прямолинейного движения учитывались силы трения и сопротивления воздуха, сила тяжести, сила тяги и сила инерции. Модель дополнена зависимостью крутящего момента от частоты вращения коленчатого вала, полученной путем аппроксимации, а также углом изменения наклона дорожного полотна. В процессе исследований установлено, что для повышения адекватности модели требуется учитывать динамику двигателя и трансмиссии. Данный недостаток устранен путем введения двух дополнительных дифференциальных уравнений первого порядка. При*