УДК 004.056.5

С.С. Велигодский, Н.Г. Милославская

Методика оценки уровня зрелости центров управления сетевой безопасностью

Представлена разработанная методика оценки уровня зрелости центров управления сетевой безопасностью (ЦУСБ) информационно-телекоммуникационных сетей. Она основана на применении унифицированной модели зрелости ЦУСБ и включает в себя следующие этапы: инициирование и подготовительные мероприятия к проведению оценки; определение возможности проведения оценки и составление плана работ; проведение оценки и формулирование обнаружений оценки; подготовка отчета об оценке и завершение проведения оценки. Данная методика предназначена для специалистов организации-владельца ЦУСБ, проводящих самооценку (самостоятельную оценку) уровня зрелости своего ЦУСБ, а также специалистов специализированных организаций, признанных компетентными для проведения профессиональной независимой оценки уровня зрелости ЦУСБ конкретной организации.

Ключевые слова: центр управления сетевой безопасностью, информационно-телекоммуникационная сеть, уровень зрелости, методика оценки уровня зрелости, лазерная подсветка, высокотемпературное горение, высоковольтный источник питания, синхронизация.

DOI: 10.21293/1818-0442-2023-26-2-31-41

Согласно 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», информационно-телекоммуникационная сеть (ИТКС) является объектом критической информационной инфраструктуры (КИИ) Российской Федерации (РФ), используемым различными субъектами КИИ – от государственных органов и учреждений до юридических лиц и индивидуальных предпринимателей [1]. В целях обеспечения информационной безопасности (ОИБ) ИТКС субъект КИИ создает и обеспечивает функционирование системы безопасности своих ИТКС на базе специального структурного подразделения [2]. В работе [3] показано, что в его составе необходимо наличие центра управления сетевой безопасностью (ЦУСБ) ИТКС.

Взяв за основу терминологию стандартов [4, 5], определим модель зрелости ЦУСБ ИТКС как структурированный набор элементов, объединяющий информационную потребность установления уровня зрелости ЦУСБ с их атрибутами – свойствами или характеристиками ЦУСБ, которые могут быть определены количественно или качественно, вручную или автоматизированными средствами. Информационная потребность – знания (сведения), необходимые для управления целями, задачами, рисками и проблемами. 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. Обеспечивающие компоненты ЦУСБ, а именно, процессы управления сетевой безопасностью (УСБ) ИТКС, предоставляемые ЦУСБ потребителям услуги по УСБ ИТКС, используемые для этого технологии, реализованные в конкретных системах и помогающие персоналу ЦУСБ обеспечивать информационную безопасность (ИБ) ИТКС и собственную ИБ, а также организационное и кадровое обеспечение, рассматриваются как направления оценки (НО) уровня зрелости ЦУСБ.

Целью статьи является представление разработанной методики оценки уровня зрелости (МОУЗ) ЦУСБ с применением ранее созданной унифицированной модели зрелости (УМЗ) ЦУСБ [6, 7].

Принципы проведения оценки уровня зрелости ЦУСБ с применением УМЗ ЦУСБ

Оценка уровня зрелости ЦУСБ представляет собой упорядоченную последовательность действий (процесс) по прямому или косвенному определению уровня зрелости ЦУСБ в пределах области оценки уровня зрелости на основе оценки его атрибутов и их сопоставления с критериями зрелости ЦУСБ как совокупности требований, характеризующих определенный уровень зрелости ЦУСБ согласно УМЗ ЦУСБ. Этот процесс должен основываться на взаимосвязанных принципах, следование которым является гарантией получения объективного заключения по итоговому уровню зрелости конкретного ЦУСБ. Такие принципы, соблюдение которых должно быть обязательным для всех участвующих в оценке сторон, делают оценку надежным средством получения повторяемых и сопоставимых результатов как основы для дальнейшего совершенствования ЦУСБ.

Определим следующие принципы проведения оценки уровня зрелости ЦУСБ (на основе [3]):

- определенность целей оценки, что обеспечит реализуемость проведения оценки;
- ориентация на использование открытых стандартов, что позволит провести оценку с учетом требований, применимых к ЦУСБ как объекту оценки стандартов, и в соответствии с лучшими практиками на современном уровне развития науки и техники;
- оценка по эталону, во время которой производится сопоставление получаемых результатов со значениями эталонной шкалы;

• системность оценки – учет взаимосвязей элементов, условий и факторов, влияющих на уровень зрелости ЦУСБ, включая собственную защищенность ЦУСБ и процессов УСБ ИТКС, осуществляемых ЦУСБ, и услуг по УСБ ИТКС, предоставляемых ЦУСБ;

• комплексность, многомерность, полнота и непрерывность оценки – сочетание и согласованная оценка всех НО ЦУСБ в рамках установленной области оценки в отношении всех критериев оценки на основе УМЗ ЦУСБ и в соответствии с поставленными целями оценки с учетом использования знаний, полученные в ходе предшествующих оценок;

• масштабируемость оценки – обеспечение возможности увеличения или уменьшения оцениваемых атрибутов объектов оценки и затрат для конкретного ЦУСБ;

• унификация и типизация (тиражируемость) оценки и ее результатов – процесс проведения оценки (кратко – процесс оценки) должен быть применим к ЦУСБ ИТКС организаций различного масштаба, подчиненности и сферы деятельности, а итоговые результаты должны быть повторяемы (воспроизводимы) и сопоставимы между собой;

• адаптивность (настраиваемость) оценки и области оценки – обеспечение гибкой настройки процесса оценки и используемых при этом средств под конкретный ЦУСБ, область оценки и требования по ОИБ применимых нормативных документов;

• достаточная формализация проведения оценки – процессы, средства, исходные данные, конечные результаты каждого этапа проведения оценки и отчетные документы должны быть детально описаны, понятны и не вызывать различных толкований;

• несекретность оценки – процессы и средства проведения оценки должны быть известными (это не распространяется на информацию ограниченного доступа, получаемую в ходе проведения оценки, например, данные типа ключей шифрования и паролей, риски ИБ, уязвимости элементов ИТКС и т.п.);

• управляемость процесса оценки и контролируемость хода ее проведения за счет единой методики ее проведения и распределенного (параллельного или последовательного) выполнения отдельных этапов оценки, что позволит своевременно выявить и устранить допущенные ошибки и случайно пропущенные действия, а также обнаружить попытки несанкционированного вмешательства в процесс и результаты оценки;

• консолидация исходных и промежуточных данных, полученных из различных источников, – объединение данных для их всестороннего совместного анализа; при этом получаемые свидетельства (данные, выкладки и т.п.) должны быть проверяемы и достоверны;

• разумная достаточность, результативность и эффективность – процесс оценки строится таким образом, чтобы гарантированно получаемый в конце оценки результат отвечал информационным потребностям всех заинтересованных сторон, для которых требуется установление уровня зрелости ЦУСБ, с учетом задаваемых ограничений на трудоемкость, финансовые затраты и используемые средства проведения оценки;

• беспристрастность (объективность) и профессиональная осмотрительность при проведении оценки – проводящий оценку компетентный и знающий специфику конкретного ЦУСБ оценщик должен быть ответственным, независимым, справедливым и непредубежденным во всех своих действиях и получаемых результатах, принимать обдуманные решения, не поддаваться любым влияниям, которые могут быть оказаны на его мнение, а также своевременно предоставлять уполномоченным сторонам информацию о ходе процесса оценки и ее результатах;

• обоснованность итогового результата оценки – результат оценки должен быть четким, полным и понятным, что должно быть отражено в отчетных материалах (заключении) о проведении оценки и подкреплено необходимыми свидетельствами.

Методика оценки уровня зрелости ЦУСБ

Под МОУЗ ЦУСБ организации как объекта оценки понимается последовательность действий, позволяющая на основе собранных качественных и количественных документированных свидетельств оценки определить уровень зрелости ЦУСБ с применением УМЗ ЦУСБ (рис. 1).

Рис. 1. Высокоуровневое представление процесса проведения оценки уровня зрелости ЦУСБ

При этом в качестве источников свидетельств оценки обычно выступают следующие источники, которые имеют отношение к критериям зрелости ИБ и могут быть проверены (адаптировано на основе [8]):

• документы и записи ЦУСБ и иные материалы ЦУСБ в бумажном или электронном виде и, при необходимости, документы третьих лиц, относящиеся к ОИБ ИТКС (например, отчеты об уязвимостях, проведенных тестированиях на проникновение, аудитах ИБ и т.п.);

• устные высказывания и письменные ответы (изложение фактов) работников ЦУСБ в процессе проводимых опросов, оформленные в виде соответствующих протоколов;

• документы и устные высказывания третьих лиц, относящиеся к функционированию ЦУСБ и ОИБ ИТКС;

• результаты наблюдений членов группы оценки за деятельностью ЦУСБ и отдельными объектами

оценки в области оценки (например, анализ данных систем мониторинга ИБ в функциональных подразделениях организации);

• параметры конфигурационных настроек средств защиты информации и программного и аппаратного обеспечения (ПО и АО) ИТКС в целом и ЦУСБ в частности;

• технические и программные средства сбора свидетельств оценки, осуществляющие анализ журналов регистрации событий (ЖРС), фактических настроек ПО и АО, сканирование на наличие уязвимостей, тестирование на проникновение и т.п.;

• иные источники типа баз данных угроз ИБ и уязвимостей, веб-сайтов по ИБ и т.п.

При разработке МОУЗ ЦУСБ ИТКС с применением УМЗ ЦУСБ использовались лучшие идеи следующих известных методик:

• методикой оценки соответствия организационных и технических мер защиты информации финансовой организации требованиями ГОСТ Р 57580.1, поскольку она устанавливает способы оценки выбора и реализации таких мер [8];

• методикой проведения аудита ИБ в организациях банковской системы РФ [9], поскольку обеспечение необходимого и достаточного уровня их ИБ требует проверки этого уровня на основе оценки соответствия ИБ организаций критериям аудита ИБ, установленным согласно требованиям СТО БР ИББС-1.0;

• руководством по аудиту систем менеджмента ИБ (СМИБ) из ГОСТ Р ИСО/МЭК 27007-2014 [10], поскольку ЦУСБ – часть СМИБ организации [3];

• руководящими указаниями по проведению аудита систем менеджмента из ГОСТ Р ИСО 19011-2021 [11], поскольку ЦУСБ является системой управления, а именно, УСБ ИТКС организации;

• лучшими практиками применения моделей зрелости, например, такими, которые описаны в работах [12–19].

Разработанная МОУЗ ЦУСБ с применением УМЗ ЦУСБ включает в себя четыре этапа (рис. 2).

Согласно логике ее разработки, она удовлетворяет всем принципам проведения оценки уровня зрелости ЦУСБ, определенным выше.

Инициирование и подготовительные мероприятия к проведению оценки

Входные данные этапа: первичная документированная информация об организации, ее ИТКС и ЦУСБ (объекте оценки), имеющая отношение к определению уровня зрелости ЦУСБ.

Действия во время этапа. Проведение оценки начинается традиционно для аналогичных видов оценки – с планирования в виде подготовки программы оценки уровня зрелости ЦУСБ и установления целевого уровня его зрелости, после чего инициируется сам процесс оценки (рис. 3).

Программа включает в себя детальный перечень (как правило, в табличном виде) мероприятий по проведению одной или нескольких оценок (в виде конкретных процедур оценки с указанием их цели и ответственных исполнителей), запланированных на конкретный период времени и направленных на достижение конкретной цели – установление текущего уровня зрелости ЦУСБ. Кроме перечисленных сведений, желательно указать, какими документами необходимо руководствоваться при проведении оценки и каким способом ее проводить (например, сплошной метод или выборка).

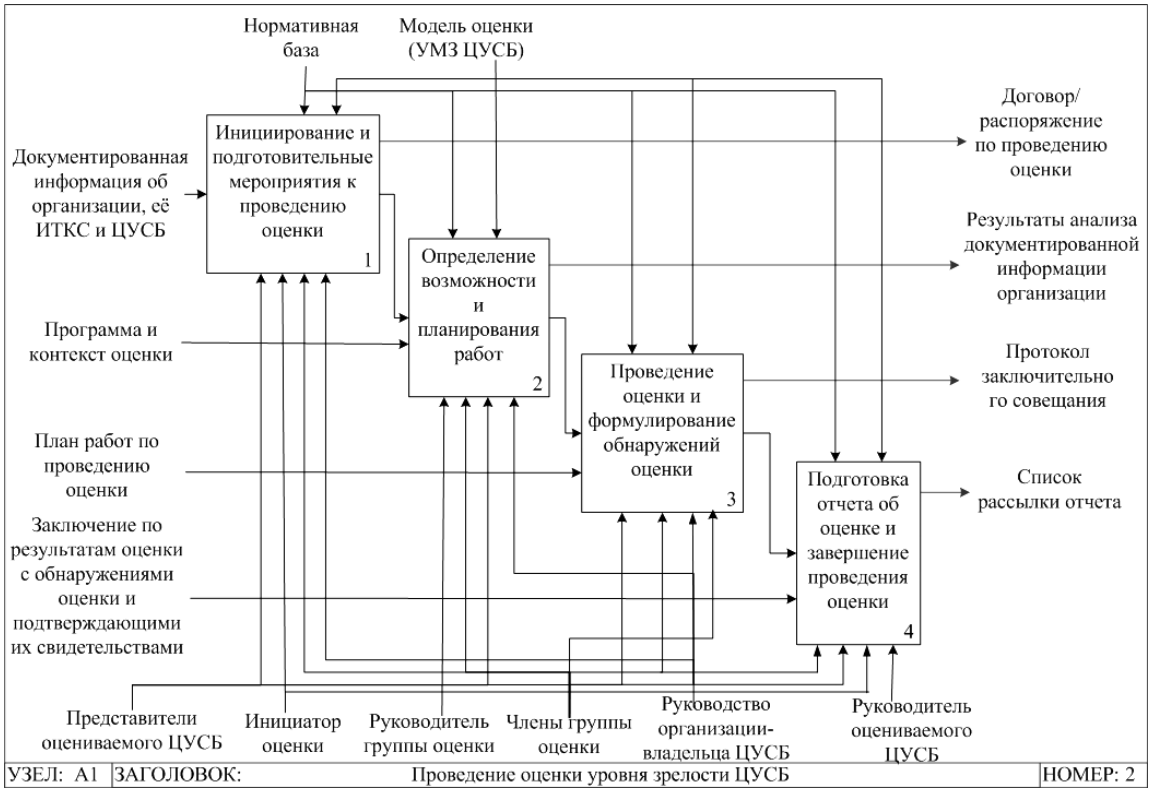

Рис. 2. Этапы проведения оценки уровня зрелости ЦУСБ

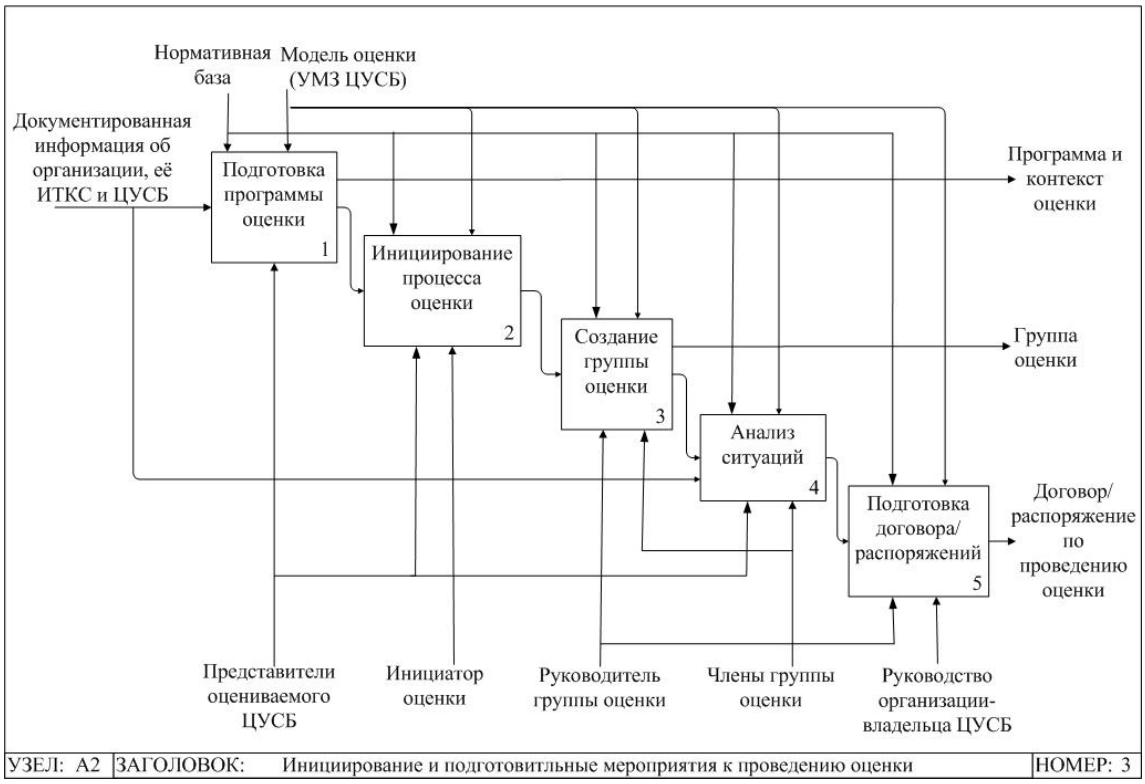

Рис. 3. Этап инициирования и подготовки

В программе отражаются как самостоятельные оценки (самооценки) уровня зрелости ЦУСБ специалистами организации-владельца ЦУСБ, так и независимые оценки, проводимые специалистами специализированных организаций, признанных компетентными для ее проведения. Она должна быть согласована с руководителем ЦУСБ и утверждена руководителем Управления безопасности организации, в структуру которого входит ЦУСБ.

Установление целевого уровня зрелости ЦУСБ осуществляется руководством организации и его Управления безопасности на основе разработанных и утвержденных документов с соответствующими требованиями к уровню зрелости, например, в рамках Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы РФ (ГосСОПКА).

Инициатором (заказчиком) проведения оценки уровня зрелости ЦУСБ может являться как сама организация, владеющая им, так и уполномоченный контролирующий орган, который имеет законное право запросить проведение такой оценки (представляется, что для субъектов КИИ процедура оценки должна стать обязательной, а контролирующий орган определен в рамках ГосСОПКА). Именно инициатор оценки определяет потребителей результатов оценки, владельцем которых является он сам.

В качестве субъекта оценки уровня зрелости ЦУСБ может выступать как сама организация-владелец ЦУСБ (в случае самооценки), так и внешняя по отношению к организации специализированная организация, созданная уполномоченным органом с целью, например, дальнейшей сертификации ЦУСБ (если для субъектов КИИ в дальнейшем будет разработано такое требование), или внутренняя группа из работников организации, проводящая оценку с целью совершенствования своего ЦУСБ или подготовки к оценке внешней группой оценки. В обоих случаях создается группа оценки, определяется и назначается ее руководитель, который несет ответственность за весь процесс оценки и формирует команду из членов группы с необходимыми квалификацией и компетенциями и распределяет основные роли и обязанности между ними.

Далее группа оценки осуществляет анализ ситуации на основе документированной информации, предоставленной организацией, и устанавливает контекст оценки, что включает цели оценки, требования к ней, потребителей результатов оценки, ее область, основные критерии, ограничения (например, степень вмешательства группы оценки в деятельность персонала и проверяемых систем), особенности, модели оценки, включая УМЗ ЦУСБ, применимые подходы и т.п. В числе прочих должны быть получены ответы на следующие вопросы: проводилась ли такая оценка ранее, если да, то что она показала; какие результаты ожидаются по завершении оценки и какие выводы могут быть сделаны на основе полученных результатов; какие необходимы человеческие, временные и иные ресурсы для проведения оценки; как будут обрабатываться получаемые в ходе проведения оценки свидетельства и т.п.

На данном этапе готовится документ – договор с внешней группой оценки или распоряжение по организации по привлечению внутренней группы оценки, в котором также указываются цель, область и критерии оценки и другие важные сведения, как минимум:

даты и продолжительность проведения оценки; порядок взаимодействия членов группы оценки и представителей ЦУСБ и ИТКС; ответственность руководства ЦУСБ и ИТКС за подготовку и предоставление необходимых свидетельств оценки; порядок сбора необходимых свидетельств оценки; порядок привлечения технических экспертов, если члены группы не обладают необходимыми знаниями и опытом по специальным вопросам, подлежащим оценке; необходимые ограничения ответственности членов группы оценки; требования к отчету об оценке и т.п.

Целью оценки уровня зрелости ЦУСБ может являться как совершенствование ЦУСБ и его переход на более высокий уровень зрелости, если инициатором проведения оценки выступает сама организация, так и, например, установление соответствия текущего уровня зрелости ЦУСБ субъекта КИИ рекомендуемому уровню зрелости для ИТКС как объекта КИИ РФ.

Область оценки уровня зрелости ЦУСБ включает в себя содержание в виде конкретных объектов оценки (весь ЦУСБ в целом и отдельные оцениваемые объекты внутри ЦУСБ) и пять НО. При этом оценивается сложность ЦУСБ и ИТКС, в состав которой он входит, наличие схожих объектов оценки и другие аспекты, влияющие на проведение оценки.

Критерии зрелости ЦУСБ, согласно УМЗ ЦУСБ, характеризуют определенный уровень зрелости ЦУСБ. Возможны два подхода: принятие эталона уровней зрелости из УМЗ ЦУСБ или установление собственных для организации и ее ЦУСБ уровней, если в силу каких-либо обстоятельств эталонные шкалы УМЗ организацию или группу оценки не устраивают. Имея эталон, необходимо сформулировать на его основе собственные критерии оценки.

Процесс оценки основан на модели оценки, согласно УМЗ ЦУСБ включающей в себя область оценки с объектами оценки и их атрибутами, методы и критерии оценки, отображение и преобразование полученных значений для атрибутов объекта оценки в показатели и результаты оценки, а также устанавливает характеристики процесса оценки в целом. Представление проведения оценки в качестве процесса показано на рис. 4, где отражены входные и выходные данные процесса, его ресурсное обеспечение с точки зрения ролей и обязанностей участвующих в процессе и управляющих воздействий в виде модели оценки (на основе [20, 21]).

Выходные данные этапа: программа и контекст оценки, договор/распоряжение по проведению оценки и группа оценки.

Определение возможности проведения оценки и составление плана работ

Входные данные этапа: программа и контекст оценки, группа оценки.

Действия во время этапа. До начала проведения оценки на основе первичной документированной информации, полученной от организации и ЦУСБ на первом этапе, группа оценки во главе с ее руководителем должна вынести обоснованное решение о достаточности ресурсов (человеческих, инструментальных средств и т.п.), данных и осуществимости (потенциальной возможности) их сбора, а следовательно, возможности проведения оценки в отведенное время, чтобы обеспечить достижение целей оценки (рис. 5). Если делается вывод, что проведение оценки в силу аргументированных обстоятельств невозможно, то руководитель группы оценки уведомляет об этом руководство организации-владельца ЦУСБ.

Если решение положительное, то необходимо составить план работ по проведению оценки. Он представляет собой подробный план с описанием того, кто участвует в процессе оценки, какие работы и в какие сроки проходят, кто несет ответственность за отдельные работы, какие ресурсы необходимы для них и т.п.

Рис. 4. Представление проведения оценки уровня зрелости ЦУСБ как процесса

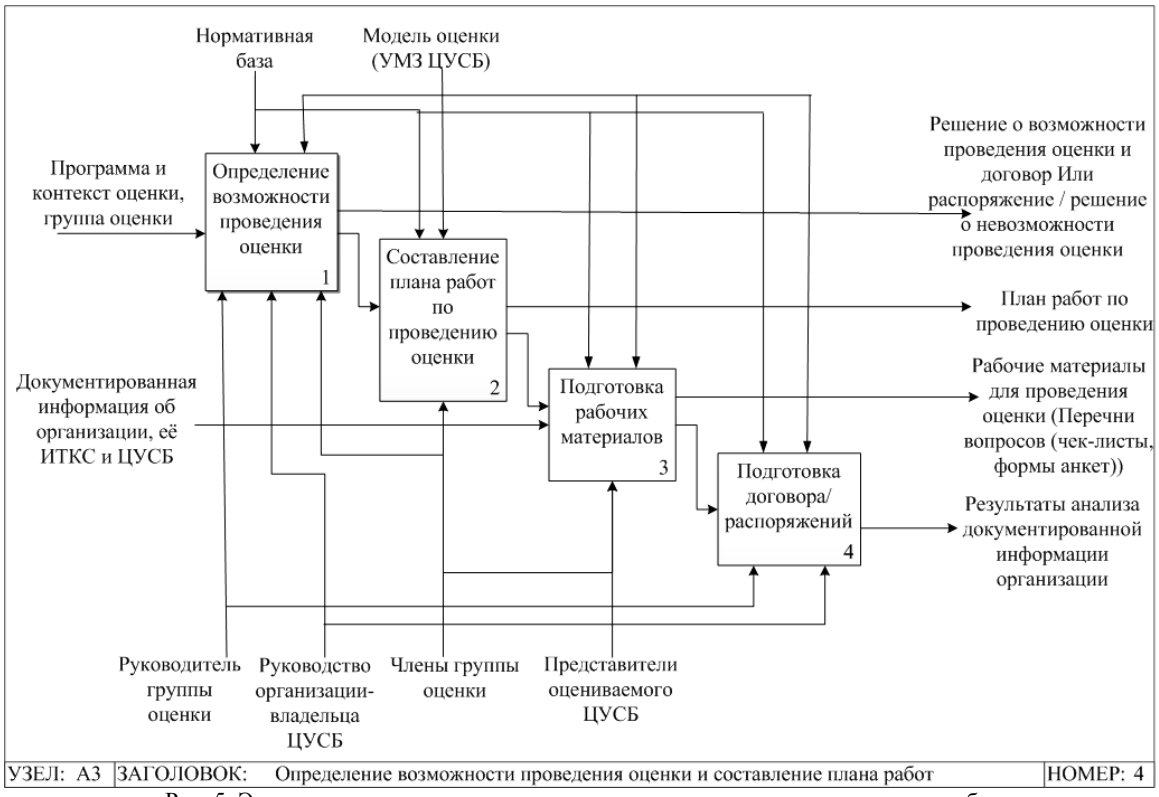

Рис. 5. Этап определения возможности проведения оценки и планирования работ

В этом плане также отражаются цель, область и критерии оценки, дополненные следующей информацией: даты и продолжительность проведения оценки; состав группы оценки; роли ее членов и представителей со стороны ЦУСБ и, возможно, подразделения, в ведении которого находится ИТКС; результаты анализа документов, предоставленных организацией в целом и ЦУСБ в частности для проведения оценки; описание конкретных работ; распределение ресурсов при проведении оценки; вопросы обеспечения конфиденциальности и надлежащего обращения с информацией, полученной во время проведения оценки, и т.д.

После этого группа оценки готовит необходимые материалы для проведения оценки (например, перечни вопросов (чек-листы, формы анкет) на бумажных или электронных носителях), устанавливает контакт с назначенными представителями оцениваемого ЦУСБ, в первую очередь для согласования способов обмена информацией, и перед началом оценки представляет руководству ЦУСБ план работ по проведению оценки и согласует его с обеих сторон.

Выходные данные этапа: результаты анализа первичной документированной информации организации; решение о возможности проведения оценки; план работ по проведению оценки; рабочие материалы для проведения оценки.

Проведение оценки и формулирование обнаружений оценки

Входные данные этапа: план работ по проведению оценки; результаты анализа первичной документированной информации организации; рабочие материалы для проведения оценки.

Действия во время этапа. Действия по проведению оценки уровня зрелости ЦУСБ (рис. 6) практически не отличаются от действий по проведению аудита, а значит, за их основу могут быть взяты положения стандартов [8–11] и поэтому изложены кратко. Основное отличие – в заполняемых формах анкет, на основе которых рассчитываются показатели уровней зрелости отдельных объектов оценки.

Перед началом проведения оценки проводится вступительное совещание с участием группы оценки и представителей самой организации и ЦУСБ с целью взаимного представления участвующих в процессе оценки сторон, краткого изложения действий по оценке, обсуждения методов проведения оценки и получения свидетельств оценки, подтверждения способов обмена информацией между сторонами и доступа к необходимой информации, а также определения действий в неординарных ситуациях.

Поскольку результаты проведения оценки основаны на анализе свидетельств оценки, то суть данного этапа заключается в сборе свидетельств оценки для оценивания объектов оценки ЦУСБ по пяти НО согласно УМЗ ЦУСБ с последующим формированием итоговой оценки сначала по пяти НО, а далее и итогового уровня зрелости ЦУСБ. Сбор, регистрация, проверка (например, актуальности, полноты и последовательности) и анализ документированной информации проводятся группой оценки в течение всего процесса проведения оценки в заранее установленные сроки и позволяют ей получить объективные свидетельства оценки из различных источников в бумажном, электронном или ином виде, используя разные методы сбора информации (устные и письмен-

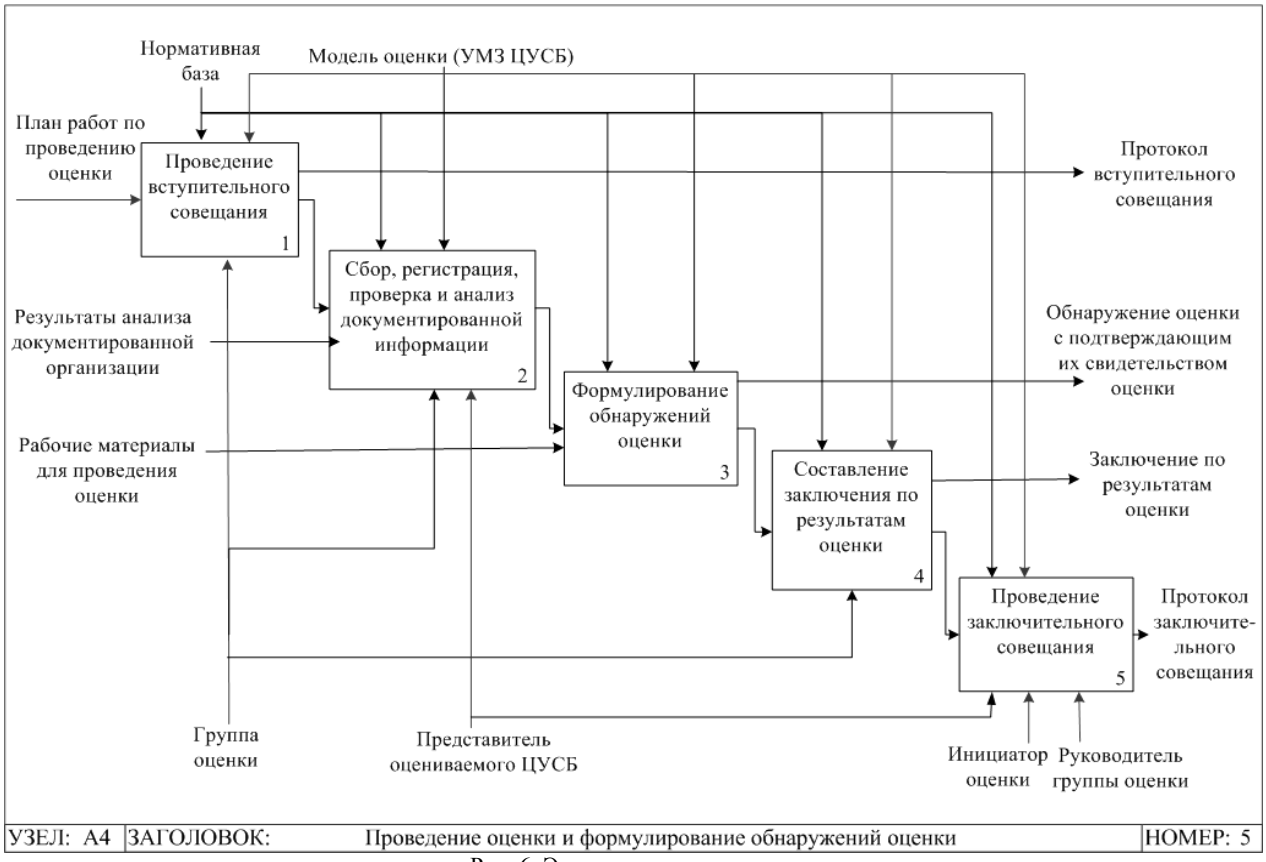

Рис. 6. Этап проведения оценки

ные опросы, наблюдения за деятельностью персонала, работой процессов и предоставлением услуг, анализ документации, репрезентативная выборка, серия испытаний, фотографирование, видеозапись, удаленный сетевой доступ и т.п.).

Выбор конкретных источников свидетельств (они перечислены ранее) осуществляет группа оценки с учетом предложений ЦУСБ и обеспечения максимальной достоверности и полноты оценки уровня зрелости ЦУСБ по пяти НО, избегая ненадлежащего вмешательства в рабочие процессы ЦУСБ. Полученные свидетельства оценки доводятся до сведения представителей ЦУСБ (для подтверждения того, что они понятны и приняты; разногласия должны быть согласованы) и вносятся в список рабочих документов оценки.

В ходе проведения оценки сначала определяются и уточняются перечни оцениваемых объектов оценки и атрибутов для них, далее на основе оценивания свидетельств оценки в соответствии с критериями оценки получаются значения для атрибутов при применении методов оценки, а полученные значения объединяются в показатели уровня зрелости с использованием соответствующих функций, как это описано в УМЗ ЦУСБ, с установленными уровнями зрелости пяти НО и ЦУСБ в целом. Обнаружения оценки (результаты оценивания собранных свидетельств оценки по отношению к критериям оценки и их интерпретация), указывающие на конкретный уровень зрелости по степени выполнения критериев оценки (попадание в конкретный интервал шкалы эталонных значений, начинающейся с «0», когда отмечается полное несоответствие критериям оценки, и заканчивающейся «1»), и обоснование всех полученных показателей для всех атрибутов объектов оценки и уровней зрелости вместе со свидетельствами оценки включают в отчет по оценке. Полученные обнаружения оценки и подтверждающие их свидетельства доводятся до сведения представителей ЦУСБ (для подтверждения того, что они понятны, верны и приняты; разногласия должны быть согласованы).

Оценка уровней зрелости пяти НО проводится сначала отдельно для каждого из них, возможно, параллельно по времени, а потом по итогам устанавливается уровень зрелости ЦУСБ как минимальный из всех рассчитанных.

Далее группа оценки составляет заключение по результатам оценки, в котором указывает полученный уровень зрелости ЦУСБ, достижение целей оценки, охват области оценки, выполнение критериев оценки и ее обнаружения. Но, в отличие от аудита ИБ, при оценке уровня зрелости ЦУСБ рекомендации по его усовершенствованию группа оценки не формулирует (во всяком случае это не является обязательным). Возможен и второй вариант заключения – отказ от его составления, в случае, когда ограничения при проведении оценки были столь существенны, что группа оценки не смогла получить достаточные свидетельства и была не в состоянии провести оценку.

Для сообщения обнаружений и результатов оценки инициатору оценки и ЦУСБ таким образом, чтобы они были поняты и признаны, проводится

заключительное совещание под председательством руководителя группы оценки. Все расхождения во мнениях относительно обнаружений и заключения обсуждаются между участниками совещания до прихода к соглашению и фиксируются в его протоколе, а нерешенные вопросы отражаются в отчете об оценке.

Выходные данные этапа: обнаружения оценки с подтверждающими их свидетельствами оценки; заключение по результатам оценки; протоколы вступительного и заключительного совещаний.

Подготовка отчета об оценке и завершение проведения оценки

Входные данные этапа: заключение по результатам оценки с обнаружениями оценки и подтверждающими их свидетельствами оценки.

Действия во время этапа. По результатам проведения оценки руководитель группы оценки готовит отчет, за содержание и весь процесс подготовки которого он несет ответственность. Отчет должен содержать полные, точные, четкие и достаточные входные и выходные данные оценки, включая следующее (при необходимости с соответствующими ссылками):

- сведения об инициаторе оценки ЦУСБ;
- сведения об оцениваемом ЦУСБ и организации-владельце;
- даты, продолжительность и места проведения оценки;
- сведения о группе оценки, ее руководителе и членах группы;
- сведения о представителях со стороны ЦУСБ;
- цель оценки;
- область оценки;
- критерии оценки;
- особенности и ограничения оценки;
- использованные подходы к оценке;
- краткое описание УМЗ ЦУСБ;
- план работ по проведению оценки с описанием конкретных мероприятий и распределением ресурсов;
- краткое изложение процесса оценки, включая возникшие проблемы, которые могут отразиться на достоверности обнаружений оценки и ограничении области оценки, а также любые неразрешенные разногласия между группой оценки и ЦУСБ/организацией-владельцем;
- список представителей ЦУСБ, которые сопровождали членов группы оценки, и список опрашиваемых группой оценки;
- подтверждение того, что цель оценки в рамках области оценки с использованием установленных критериев оценки и в соответствии с планом оценки достигнута;
- обнаружения оценки с подтверждающими их свидетельствами оценки;
- выявленная положительная/отрицательная динамика, если оценка проводилась ранее;
- заключение по результатам оценки;
- план последующих действий, если таковые требуются;
- вопросы обеспечения конфиденциальности и надлежащего обращения со всей информацией, полученной во время оценки, и заявление о конфиденциальном характере содержания отчета (за исключением случаев, прямо предусмотренных действующим законодательством РФ);
- документально оформленная совокупность свидетельств оценки;
- опись прилагаемых бумажных документов (с копиями) и машинных носителей, на которых содержатся использованные в ходе проведения оценки документы в электронном виде, с указанием их реквизитов;
- лист рассылки отчета.

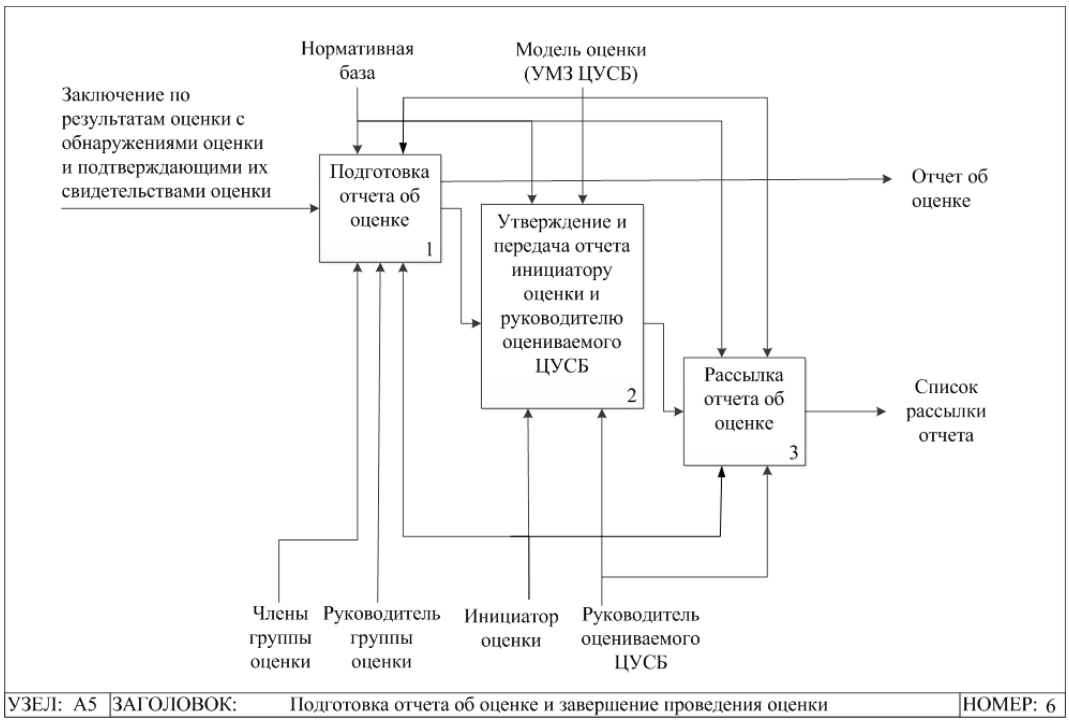

Рис. 7. Этап завершения проведения оценки

Отчет об оценке, являющийся собственностью инициатора оценки, подписывается членами группы оценки, утверждается ее руководителем и выпускается в согласованные сроки (в противном случае причины задержки доводятся до сведения инициатора оценки и ЦУСБ). Далее он подлежит передаче инициатору оценки и оцениваемому ЦУСБ с последующей рассылкой иным сторонам, определенным в договоре или распоряжении по оценке. При этом необходимо предусмотреть соответствующие меры по обеспечению его конфиденциальности.

Оценка завершена (рис. 7), когда все запланированные мероприятия выполнены или достигнуто иное соглашение с инициатором оценки (например, в случае непредвиденных обстоятельств, которые мешают завершению оценки в соответствии с планом), а отчет передан инициатору оценки.

Выходные данные этапа: отчет об оценке; список рассылки отчета.

Заключение

Представлена разработанная МОУЗ ЦУСБ, которая основана на применении ранее созданной авторами статьи УМЗ ЦУСБ. Данная методика предназначена для специалистов организации-владельца ЦУСБ, проводящих самооценку уровня зрелости своего ЦУСБ, а также специалистов специализированных организаций, признанных компетентными для проведения профессиональной независимой оценки уровня зрелости ЦУСБ конкретной организации. В продолжение исследования необходимо разработать формы анкет для заполнения для оценки уровня зрелости всех объектов оценки в рамках каждого НО уровня зрелости ЦУСБ.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации [ФЗ от 26 июля 2017 г. № 187-ФЗ: принят Гос. думой 12 июля 2017 г.; одобрен Советом Федерации 19 июля 2017 г.]. – 2017. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201707260023, свободный (дата обращения: 12.06.2023).

2. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». – 2022. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202205010023, свободный (дата обращения: 12.06.2023).

3. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. – М.: Горячая линия-Телеком, 2021. – 431 с.

4. ISO/IEC/IEEE 15939:2017 Systems and software engineering – Measurement process. – 2017. – Режим доступа: https://www.iso.org/standard/71197.html, свободный (дата обращения: 12.06.2023).

5. ГОСТ Р ИСО/МЭК 27004–2021. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. – Введ. 30.11.2021. – М.: Стандартинформ, 2021. – 46 с.

6. Велигодский С.С. Подход к оценке уровня зрелости центров управления сетевой безопасностью / С.С. Велигодский, Н.Г. Милославская // Системы высокой доступности. – 2023. – Т. 19, № 2. – С. 25–37. DOI: 10.18127/j20729472-202302-02.

7. Велигодский С.С. Технологии, обеспечивающие функционирование центров управления сетевой безопасностью информационно-телекоммуникационных сетей, и оценка уровня их зрелости / С.С. Велигодский, Н.Г. Милославская // Вестник современных цифровых технологий. – 2023. – №. 15. – С. 30–41.

8. ГОСТ Р 57580.2–2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. – Введ. 28.03.2018. – М.: Стандартинформ, 2018. – 23 с.

9. СТО БР ИББС-1.1–2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности. – М: Банк России, 2007. – Введ. 01.05.2007. – 14 с.

10. ГОСТ Р ИСО/МЭК 27007–2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. – Введ. 01.06.2015. – М.: Стандартинформ, 2019. – 24 с.

11. ГОСТ Р ИСО 19011–2021 Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента. – Введ. 01.07.2021. – М.: Стандартинформ, 2021. – 36 с.

12. Gardiner M. The Critical Incident Response Maturity Journey / M. Gardiner [Электронный ресурс]. – EMC Corporation, 2013. – Режим доступа: http://docs.media. bitpipe.com/io_11x/io_115661/item_894499/Critical%20Incident%20Response%20Maturity.pdf, свободный (дата обращения: 12.06.2023).

13. SIM3: Security Incident Management Maturity Model [Электронный ресурс]. – Open CSIRT Foundation, 2019. – Режим доступа: http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf, свободный (дата обращения: 12.06.2023).

14. Dorofee A. Incident Management Capability Assessment / A. Dorofee, R. Ruefle, M. Zajicek, D. McIntire, C. Alberts, S. Perl, C.L. Huth, P. Walters [Электронный ресурс]. – Software Engineering Institute of Carnegie Mellon University, 2018. – Режим доступа: https://resources.sei.cmu.edu/asset_files/TechnicalReport/ 2018_005_001_538866.pdf, свободный (дата обращения: 12.06.2023).

15. State of security operations [Электронный ресурс]. – Hewlett-Packard, 2014. – Режим доступа: http://h41382.www4.hpe.com/gfs-shared/downloads-303.pdf, свободный (дата обращения: 12.06.2023).

16. Os V.R. SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers [Электронный ресурс]. – Luleå University of Technology, 2016. – Режим доступа: http://www.diva-portal.org/smash/get/diva2:1033727/FULLTEXT02.pdf, свободный (дата обращения: 12.06.2023).

17. Nettitude Blog: Cybersecurity Maturity Assessments Explained [Электронный ресурс]. – Nettitude, 2020. – Режим доступа: https://blog.nettitude.com/cyber-maturity-assessments-explained-nettitude, свободный (дата обращения: 12.06.2023).

18. Crump J. Security Operations Center – Use Case Maturity Model/Cube (SOC-UCMM) [Электронный ресурс]. – 2018. – Режим доступа: https://www.jeffreydoncrump.com/post/security-operations-centre-soc-managed-security-service-provider-monitoring-content-maturity-cube, свободный (дата обращения: 12.06.2023).

19. The Security Operations Maturity Model: A Practical Guide to Assessing and Improving the Capabilities of Your

Security Operations Center [Электронный ресурс]. – LogRhythm, 2019. – Режим доступа: https://logrhythm.com/security-operations-maturity-model-white-paper/, свободный (дата обращения: 12.06.2023).

20. ГОСТ Р ИСО/МЭК 33002–2017. Информационная технология. Оценка процесса. Требования к проведению оценки процесса. – Введ. 01.03.2018. – М.: Стандартинформ, 2017. – 16 с.

21. Аудит информационной безопасности / под ред. А.П. Курило. – М.: БДЦ-Пресс, 2006. – 304 с.

Велигодский Сергей Сергеевич
Инженер Института интеллектуальных кибернетических систем Национального исследовательского ядерного университета МИФИ (НИЯУ МИФИ)
Каширское ш., 31, г. Москва, Россия, 115409
Тел.: +7-926-386-84-00
Эл. почта: SSVeligodsky@sberbank.ru

Милославская Наталья Георгиевна
Д-р техн. наук, доцент, проф. НИЯУ МИФИ
Каширское ш., 31, г. Москва, Россия, 115409
ORCID: 0000-0002-1231-1805
Тел.: +7-916-677-65-99
Эл. почта: NGMiloslavskaya@mephi.ru

Veligodskiy S.S., Miloslavskaya N.G.

Methodology for assessing the maturity level of network security centers

The developed methodology for assessing the maturity level of Network Security Centers (NSCs) for information and telecommunication networks is presented. It is based on the application of the unified NSC maturity model and includes the following steps: assessment initiation and preparatory activities; determining the possibility of an assessment and drawing up a work plan; assessment itself and formulating assessment findings; preparation of the assessment report and assessment completion. This methodology is intended for specialists of a NSC owner organization, who conduct a self-assessment of its NSC maturity level, as well as specialists of specialized organizations recognized as competent to conduct a professional independent assessment of the maturity level of the NSC of a particular organization.

Keywords: network security center, information and telecommunication network, maturity level, methodology for assessing the maturity level.
DOI: 10.21293/1818-0442-2023-26-2-31-41

References

1. Federal Law No. 187-FZ dated 26.07.2017. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii [On the Security of the Critical Information Infrastructure of the Russian Federation]. 2017. Available at: http://publication.pravo.gov.ru/Document/View/0001201707260023, free. (Accessed: June 12, 2023) (in Russ.).

2. Decree of the President of the Russian Federation No. 250 dated 01.05.2022 O dopolnitel'nykh merakh po obespecheniyu informatsionnoy bezopasnosti Rossiyskoy Federatsi» [On Additional Measures to Ensure the Information Security of the Russian Federation]. 2022. Avilable at: http://publication.pravo.gov.ru/Document/View/ 0001202205010023, free. (Accessed: June 12, 2023) (in Russ.).

3. Miloslavskaya N.G. *Nauchnyye osnovy postroyeniya tsentrov upravleniya setevoy bezopasnost'yu v informatsionno-telekommunikatsionnykh setyakh* [Scientific Foundations for Building Network Security Centers in Information and Telecommunication Networks]. Moscow, Hot Line-Telecom, 2021. 431 p. (in Russ.).

4. ISO/IEC/IEEE 15939:2017 Systems and Software Engineering – Measurement Process. 2017. Available at: https://www.iso.org/standard/71197.html, free (Accessed: June 12, 2023).

5. GOST R ISO/IEC 27004–2021. Informatsionnyye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Menedzhment informatsionnoy bezopasnosti. Monitoring, otsenka zashchishchennosti, analiz i otsenivaniye [Information Technology. Security Techniques. Information Security Management. Monitoring, Measurement, Analysis and Evaluation]. Moscow, Standartinform, 2021, 46 p. (in Russ.).

6. Veligodskiy S.S., Miloslavskaya N.G. [Approach to Assessing Network Security Centers' Maturity Level]. *Highly Available Systems,* 2023, vol. 19, no. 2, pp. 25–37. DOI: https://doi.org/10.18127/j20729472-202302-02 (in Russ.).

7. Veligodskiy S.S., Miloslavskaya N.G. [Technologies Ensuring the Operation of Network Security Centers of Information and Telecommunication Networks and their Maturity Level Assessment]. *Journal of Modern Digital Technologies,* 2023, no. 15, pp. 30–41 (in Russ.).

8. GOST R 57580.2–2018 Bezopasnost' finansovykh (bankovskikh) operatsiy. Zashchita informatsii finansovykh organizatsiy. Metodika otsenki sootvetstviya [Security of Financial (Banking) Operations. Information Protection of Financial Organizations. Conformity Assessment Methods]. Moscow, Standartinform, 2018, 23 p. (in Russ.).

9. STO BR IBBS-1.1–2007 Obespecheniye informatsionnoy bezopasnosti organizatsiy bankovskoy sistemy Rossiyskoy Federatsii. Audit informatsionnoy bezopasnosti [Information Security of Russian Banking Institutions. Information Security Audit]. Moscow, 2007, 14 p. (in Russ.).

10. GOST R ISO/IEC 27007–2014. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Rukovodstva po auditu sistem menedzhmenta informatsionnoy bezopasnosti [Information Technology. Security Techniques. Guidelines for Information Security Management Systems Auditing]. Moscow, Standartinform, 2019, 24 p. (in Russ.).

11. GOST R ISO 19011–2021. Otsenka sootvetstviya. Rukovodyashchiye ukazaniya po provedeniyu audita sistem menedzhmenta [Conformity Assessment. Guidelines for Auditing Management Systems]. Moscow, Standartinform, 2021, 36 p. (in Russ.).

12. 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, free (Accessed: June 12, 2023).

13. SIM3: Security Incident Management Maturity Model. Open CSIRT Foundation, 2019. Available at: http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mk XVIIIc.pdf (Accessed: June 12, 2023).

14. 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, free (Accessed: June 12, 2023).

15. State of security operations. Hewlett-Packard, 2014. Available at: http://h41382.www4.hpe.com/gfs-shared/downloads-303.pdf, free (Accessed: June 12, 2023).

16. Os V.R. SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers. Luleå University of Technology, 2016. Available at: http://www.diva-portal.org/smash/get/diva2:1033727/FULLTEXT02.pdf, free. (Accessed: June 12, 2023).

17. Nettitude Blog: Cybersecurity Maturity Assessments Explained. Nettitude, 2020. Available at: https://blog.nettitude.com/cyber-maturity-assessments-explained-nettitude (Accessed: June 12, 2023).

18. 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: June 12, 2023).

19. 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: June 12, 2023).

20. GOST R ISO/IEC 33002–2017. Informatsionnyye tekhnologii. Otsenka protsessa. Trebovaniya k provedeniyu otsenki protsessa [Information Technology. Process Assessment. Requirements for Performing Process Assessment]. Moscow, Standartinform, 2017. 16 p. (in Russ.).

21. *Audit informatsionnoy bezopasnosti* [Information Security Audit]. Ed. A.P. Kurilo. Moscow: BDC-Press, 2006, 304 p. (in Russ.).

Sergey S. Veligodskiy
Engineer, Institute of Intelligent Cybernetic Systems,
National Research Nuclear University
Moscow Engineering Physics Institute (MEPhI)
31, Kashirskoye sh., Moscow, Russia, 115409
Phone: +7-926-386-84-00
Email: SSVeligodsky@sberbank.ru

Natalia G. Miloslavskaya
Doctor of Science in Engineering, Associate Professor,
Professor, Institute of Intelligent Cybernetic Systems,
National Research Nuclear University MEPhI
31, Kashirskoye sh., Moscow, Russia, 115409
ORCID: 0000-0002-1231-1805
Phone: +7-916-677-65-99
Email: NGMiloslavskaya@mephi.ru