ВОЕННАЯ БЕЗОПАСНОСТЬ И НАЦИОНАЛЬНАЯ ОБОРОНА

УДК 519.812
DOI 10.37468/2307-1400-2025-4-18-28

Анализ подходов к оценке деятельности подразделений информационных технологий и связи силовых структур

Аскеров Роман Айвазович[1]

[1]Главное управление МЧС России по Ханты-Мансийскому автономному округу - Югре, г. Ханты-Мансийск, Россия

Аннотация
Актуальность исследования обусловлена возрастающей зависимостью силовых структур от информационно-телекоммуникационных систем, необходимостью объективного контроля эффективности подразделений информационных технологий и связи. Цель работы: сравнительный анализ существующих подходов к оценке деятельности подразделений информационных технологий и связи силовых структур с выявлением их достоинств, ограничений и перспектив адаптации к специфике силовых структур. В статье представлена типология подходов, включающая базовые методологии управления ИТ-сервисами (ITIL, COBIT), модели зрелости ИТ-процессов, системы ключевых показателей эффективности (KPI), специализированные стандарты и методы экспертных оценок. Выявлены общие недостатки существующих подходов (слабая связь технологических метрик с оперативными результатами, недостаточный учет условий активного противодействия). Значимость исследования заключается в формировании систематизированной научной основы для дальнейших разработок в области методического обеспечения оценки деятельности ИТ-подразделений силовых структур. Практическая значимость состоит в возможности использования выявленных достоинств и недостатков проанализированных подходов при разработке ведомственных методических документов и автоматизированных систем мониторинга деятельности ИТ-подразделений. Перспективы дальнейших исследований связаны с разработкой комплексной модели оценки деятельности ИТ-подразделений силовых структур, интегрирующей технологические метрики с показателями оперативной эффективности на всех уровнях управления.

Ключевые слова: оценка деятельности, информационные технологии, связь, силовые структуры, ключевые показатели эффективности, IT-подразделения, методы оценки.

Введение

В современных силовых структурах России информационные технологии и системы связи силовых структур играют критически важную роль в обеспечении оперативной деятельности и выполнении задач национальной безопасности. Подразделения информационных технологий и связи (далее ИТ-подразделения) становятся системообразующим элементом инфраструктуры органов внутренних дел и иных силовых ведомств, непосредственно влияя на качество управления силами и средствами силовых структур, оперативность передачи данных

и защищенность информационного пространства. В данных условиях перед руководством силовых ведомств встает задача обоснованной оценки эффективности ИТ-подразделений.

Актуальность исследования обусловлена рядом взаимосвязанных факторов. Во-первых, устойчивый рост зависимости силовых структур от информационно-телекоммуникационных систем обусловливает повышенные требования к надежности, производительности и защищенности ИТ-инфраструктуры. Сбои в работе систем связи и автоматизации непосредственно влекут снижение боеготовности и управляемости подразделений. Во-вторых, существенное увеличение объема финансирования на ИТ-нужды силовых ведомств порождает необходимость объективного контроля эффективности расходования ресурсов и оценки отдачи от инвестиций в технологическое развитие. В-третьих, специфика деятельности силовых структур (включая режим секретности, строгая иерархия, высокие требования к надежности и отказоустойчивости) существенно ограничивает возможность прямого применения подходов оценки ИТ-деятельности, применяемых, например, для коммерческих организаций.

Несмотря на широкую разработанность проблематики оценки ИТ-подразделений в гражданском секторе, применительно к силовым структурам данная область характеризуется проблемой отсутствия унифицированных методических подходов, слабой формализацией показателей эффективности, недостаточным учетом специфики организации силовых структур. Таким образом, актуальность исследования обусловлена потребностью формирования единой системы моделей и методов оценки, позволяющей количественно сравнивать эффективность ИТ-подразделений силовых структур.

В зарубежной научной литературе вопросы оценки деятельности военных ИТ-структур рассматривались, например, в работах [1-3], в отечественной науке данная проблематика нашла отражение в трудах [4, 5]. Однако комплексного систематического анализа подходов к оценке деятельности ИТ-подразделений силовых структур в научной литературе не представлено.

Целью исследования является анализ существующих подходов (модели, методы, методики) по оценке деятельности ИТ-подразделений с целью выявления их достоинств, ограничений и перспектив адаптации к специфике силовых структур.

Методы исследования

Методологическую основу исследования составляет совокупность общенаучных и специальных методов, обеспечивающих комплексное изучение предмета исследования.

Системный анализ применяется для рассмотрения ИТ-подразделений силовых структур как сложных организационно-технических систем, функционирующих в условиях жестких операционных ограничений и высокой неопределенности. Системный подход позволяет учитывать взаимосвязи между организационными, техническими и человеческими составляющими ИТ-подразделений, а также их взаимодействие с внешней средой.

Систематический обзор литературы применяется в качестве основного метода сбора и обобщения научных данных. Поиск источников осуществлялся в электронных базах данных Web of Science, Scopus, Google Scholar, РИНЦ.

Сравнительный анализ используется для сопоставления различных подходов, моделей и методик оценки деятельности ИТ-подразделений по ряду критериев.

Метод классификации применяется для структурирования изученных подходов по ключевым признакам. Разработанная типология охватывает четыре основных класса подходов: общие методологии управления ИТ-сервисами; модели зрелости ИТ-процессов; специализированные военные концепции и стандарты; интегральные и балансированные методики оценки.

Метод экспертных оценок используется в части анализа практической применимости рассматриваемых подходов. Данный метод реализован через изучение отчетов и аналитических материалов профильных экспертных организаций, а также публичных оценок со

стороны руководства ИТ-подразделений силовых ведомств, зафиксированных в открытых источниках.

Таким образом, применяемый методологический инструментарий обеспечивает репрезентативность выборки источников, системность и объективность анализа, а также возможность формулирования обоснованных выводов относительно существующего состояния методической базы оценки деятельности ИТ-подразделений силовых структур.

Аналитическая часть

1. Базовые методологии управления ИТ-сервисами

Наиболее широко применяемой в мировой практике методологией управления ИТ-сервисами является ITIL (Information Technology Infrastructure Library). Данная библиотека передового опыта, разработанная при поддержке правительства Великобритании и впоследствии получившая международное признание, представляет собой совокупность рекомендаций по организации управления жизненным циклом ИТ-сервисов [6]. В разрезе оценки деятельности ITIL предлагает систему метрик, охватывающих четыре ключевых направления: доступность сервисов, производительность, надежность и безопасность. Последняя редакция ITIL 4 (2019) существенно расширила концептуальную базу, включив принципы гибкой разработки, бережливого производства и DevOps, что обусловило более широкое применение методологии в различных отраслях.

Однако применение ITIL в силовых структурах сопряжено с рядом специфических ограничений. Методология разрабатывалась преимущественно для коммерческого сектора и ориентирована на достижение бизнес-ценности, что затрудняет ее прямую адаптацию к условиям силовых структур, где приоритетом является боеготовность подразделений, а не коммерческая эффективность. Ряд исследователей (в частности [7]) указывают на необходимость существенной модификации структуры показателей ITIL применительно к государственному сектору. В отношении силовых структур данная проблема усугубляется режимом секретности, не позволяющим в полной мере использовать данный подход.

Еще одним инструментом, относящимся к общей методологии управления ИТ-сервисами, является COBIT (Control Objectives for Information and Related Technologies). COBIT – это система управления и аудита ИТ, разработанная Ассоциацией аудита и контроля информационных систем (ISACA). COBIT ориентирован, прежде всего, на обеспечение соответствия ИТ-деятельности стратегическим целям организации, управление рисками и соблюдение нормативных требований [9, 10]. Модель COBIT 2019 предлагает 40 целей управления, объединенных в пять групп, и систему из нескольких сотен ключевых показателей деятельности (KPI) и ключевых показателей целей (KGI). Применительно к силовым структурам COBIT представляет интерес в части управления информационной безопасностью, соответствия нормативным требованиям и управления рисками. Тем не менее, как и в случае с ITIL, данная методология ориентирована в большей степени на корпоративный сектор ограничивает ее непосредственную применимость в деятельности силовых стуктур. Применительно к силовым структурам использование ITIL и COBIT наиболее целесообразно при оценке деятельности подразделений, отвечающих за повседневную эксплуатацию тыловых, кадровых, финансово-экономических и административных систем.

2. Модели зрелости ИТ-процессов

Следующим подходом к оценке деятельности ИТ-подразделений являются модели зрелости, позволяющие оценить не только текущее состояние ИТ-процессов, но и потенциал их развития [10, 11]. Наиболее известной является комплексная модель зрелости и совершенствования процессов (CMMI – Capability Maturity Model Integration), разработанная Институтом программной инженерии Университета Карнеги–Меллона по заказу Министерства обороны США [12]. В модели CMMI выделяется пять уровней зрелости: начальный (непредсказуемые процессы), управляемый (проекто-ориентированные процессы), опреде-

ленный (стандартизированные процессы), количественно управляемый (измеримые процессы) и оптимизирующий (непрерывное совершенствование). Изначально модель CMMI создавалась именно для военного применения, прежде всего для оценки зрелости разработки программного обеспечения в рамках государственных оборонных заказов. Данный фактор обусловливает ее высокую адаптированность к условиям силовых структур.

В сфере управления ИТ-сервисами широко применяется модель зрелости управления услугами (IT Service Management Maturity Model), разработанная на базе ITIL [13, 14]. Данная модель позволяет оценить зрелость ключевых ИТ-процессов, (управление инцидентами, проблемами, изменениями, конфигурациями) по пятибалльной шкале и определить приоритетные направления развития. Применительно к силовым структурам Данная модель нашла применение при проведении внутреннего аудита ИТ-служб в ряде армий государств – членов НАТО.

Одной из разновидностей данного подхода является специализированная модель зрелости NATO C2MM, разработанная для оценки способностей командования и управления воинских формирований [15, 16]. Данная модель позволяет увязать уровень развития ИТ-инфраструктуры с оперативными возможностями воинских формирований.

3. Оценка ИТ-подразделений на основе системы показателей

Концепция сбалансированной системы показателей (Balanced Scorecard, BSC), предложенная Р. Капланом и Д. Нортоном [17, 18], нашла широкое применение в оценке деятельности ИТ-подразделений как в коммерческом, так и в государственном секторе. В рамках данного подхода деятельность ИТ-подразделения рассматривается в четырех взаимосвязанных направлениях: финансовое (или ресурсная эффективность для некоммерческих организаций), клиентское (качество ИТ-сервисов с точки зрения пользователей), процессное (эффективность внутренних ИТ-процессов) и возможность развития (компетенции персонала, инновационный потенциал). В исследовании [19] авторы представили адаптированную версию данного подхода под военные организации. Ключевым отличием модифицированной версии является замена финансовой эффективности на показатели боеготовности, что позволило сфокусировать систему показателей на приоритетных для силовых структур целях.

Также применение данного подхода легло в основу реестра стандартов и профилей информационных технологий Министерства обороны США (DISR) [20]. Однако ряд исследователей отмечают существенные ограничения данного подхода, заключающиеся в трудности количественного измерения ряда перспектив развития, риск разрыва между стратегическими показателями и оперативной реальностью, а также высокую ресурсоемкость разработки и сопровождения системы показателей [21, 22].

Методики оценки деятельности ИТ-подразделений на основе ключевых показателей эффективности (KPI – Key Performance Indicators) получили широкое распространение как в коммерческом, так и в государственном секторе. В работе [23] предложена система KPI для ИТ-подразделений, охватывающая следующие области: управление инцидентами (среднее время обнаружения инцидентов, среднее время восстановления сервиса, доля инцидентов, решенных в рамках первой линии поддержки), управление изменениями (доля успешных изменений, количество срочных изменений), управление доступностью (коэффициент доступности критических систем, индекс устойчивости сервисов), управление информационной безопасностью (количество инцидентов безопасности, время обнаружения и реагирования на угрозы), а также управление персоналом (укомплектованность, уровень квалификации, текучесть кадров). В исследовании [24] предложена система KPI ИТ-подразделения, ориентированная на внедрение и интеграцию ИТ-решений, реализованная в виде дашбордов, позволяющих руководителю и сотрудникам отслеживать текущее состояние KPI и оперативно устранять отклонения.

Применительно к силовым структурам система KPI претерпевает существенные модификации. В частности, исследования, проведенные в рамках программы NATO

Communications and Information Agency (NCIA) [25], выявили необходимость дополнения стандартного набора KPI специализированными показателями, отражающими военную специфику: степень защищенности критических систем от кибератак, готовность систем связи в полевых условиях, уровень операционной совместимости, а также показатели, характеризующие производительность ИТ-систем в условиях противодействия.

4. Специализированные стандарты

Следующим для оценки деятельности ИТ-подразделений является подход, основанный на различного рода специализированных стандартах. Стандарт ISO/IEC 27001 и связанные с ним стандарты серии ISO/IEC 2700x представляют собой международно признанную основу для оценки состояния информационной безопасности, являющейся одним из ключевых аспектов деятельности ИТ-подразделений силовых структур [26, 27]. Ряд государств адаптировали требования данных стандартов к условиям военных ведомств, создав специализированные классификационные схемы и процедуры аккредитации ИТ-систем [28, 29]. В Российской Федерации аналогичную функцию выполняют требования ФСТЭК России и ФСБ России, предъявляемые к информационным системам, обрабатывающим сведения, составляющие государственную тайну.

5. Качественно-количественные метрики и экспертные оценки

Методы экспертной оценки предполагают привлечение специалистов для оценивания работы подразделений по заранее заданным критериям. Используется комбинация качественных и количественных показателей. Например, экспертами могут оцениваться уровень готовности и мотивации личного состава подразделения, а затем их совокупность переводится в балльную шкалу. В работе [30] описывается метод экспертной интуитивно-логической обработки, где группы экспертов присваивают весовые коэффициенты факторам эффективности подразделений связи. Достоинство такого подхода состоит в учете специфических особенностей силовых структур и экспертного опыта, а к недостаткам можно отнести высокие временные затраты и субъективность суждений, которые усложняют объективное сравнение между разными подразделениями.

В отечественной науке и практике вопросы оценки деятельности ИТ-подразделений силовых структур разрабатывались преимущественно в контексте управления военными системами связи и автоматизированными системами управления войсками (АСУВ). Методологические подходы к оценке эффективности АСУВ, базирующиеся на теории исследования операций и системном анализе, изложены в работах Цыганкова В.Д., Буренка В.И., Харченко В.П. [18]. Принципиальной особенностью отечественных подходов является ориентация на показатели боевой эффективности систем управления, связанные с вероятностными и временными характеристиками процессов информационного обмена. В частности, используются такие показатели, как вероятность своевременного доведения командной информации, коэффициент готовности систем связи, пропускная способность информационных каналов.

В системе силовых структур Российской Федерации оценка деятельности подразделений информационных технологий и связи традиционно осуществляется на основе проверок и инспекций, охватывающих состояние материально-технической базы, уровень подготовки личного состава и выполнение плановых показателей технического обслуживания. В последние годы в связи с масштабной цифровизацией военного управления отмечается возрастание интереса к применению современных ИТ-методологий (прежде всего ITIL и COBIT) в адаптированном виде. Вместе с тем данное направление остается недостаточно разработанным в научной литературе, что подтверждает актуальность проводимого исследования.

Сравнительный анализ рассмотренных подходов

Проведенный обзор позволяет сформировать сравнительную характеристику рассмотренных подходов по ряду ключевых критериев, представленную в Таблице 1.

Таблица 1 – Сравнительная характеристика подходов к оценке деятельности ИТ-подразделений силовых структур

Подход	Методологическая основа	Ключевые преимущества	Недостатки подхода
1. Базовые методологии управления ИТ-сервисами **(ITIL, COBIT)**	Управление жизненным циклом ИТ-сервисов; процессный подход; управление рисками и соответствием нормативным требованиям	Международное признание и широкая апробация; развитая система метрик (доступность, производительность, надежность, безопасность); интеграция с принципами Agile и DevOps (ITIL 4); пригодность для оценки тыловых и административных ИТ-систем	Ориентация на коммерческий сектор (бизнес-ценность); несовместимость с режимом секретности и закрытостью данных; необходимость существенной модификации для применения в силовых структурах; отсутствие показателей оценки в условиях активного противодействия
2. Модели зрелости ИТ-процессов	Уровневая оценка зрелости ИТ-процессов (5 уровней); выявление потенциала развития; теория управления процессами	Оценка не только текущего состояния, но и потенциала развития; обеспечивает связь уровня ИТ с оперативными возможностями; применимость для внутреннего аудита ИТ-служб	Высокая ресурсоемкость оценочных мероприятий; длительность цикла оценки не соответствует темпу оперативной деятельности; слабая адаптированность к отечественным силовым структурам
3. Оценка ИТ-подразделений на основе системы показателей **(BSC, KPI)**	Многомерная система сбалансированных показателей (финансовая, клиентская, процессная перспективы, перспектива развития); стратегическое целеполагание	Комплексный охват деятельности подразделения; возможность адаптации финансовой перспективы на показатели боеготовности; операциональность и измеримость KPI; возможность мониторинга в режиме реального времени через дашборды	Трудность количественного измерения перспективы обучения и развития; риск разрыва между стратегическими показателями и оперативной реальностью; высокая ресурсоемкость разработки и сопровождения; стандартные наборы KPI требуют существенного дополнения военно-специфическими показателями (киберустойчивость, совместимость в полевых условиях)
4. Специализированные стандарты **(ISO/IEC 27001, ФСТЭК, ФСБ)**	Нормативно-правовое регулирование в области информационной безопасности; требования к защите государственной тайны; аккредитация и сертификация ИТ-систем	Международное признание и обязательность применения; детальная регламентация требований к защите информации; адаптируемость к условиям силовых структур (специализированные классификационные схемы); наличие отечественной нормативной базы (ФСТЭК, ФСБ), учитывающей	Охват только аспекта информационной безопасности при игнорировании других направлений деятельности ИТ-подразделений; статичность требований стандартов в условиях динамично меняющегося ландшафта угроз; сложность подтверждения соответствия в части засекреченных систем; отсутствие метрик оперативной эффективности

Подход	Методологическая основа	Ключевые преимущества	Недостатки подхода
		специфику силовых структур РФ	
5. Качественно-количественные метрики и экспертные оценки	Экспертно-аналитические методы (интуитивно-логическая обработка, весовые коэффициенты); комбинирование качественных и количественных показателей	Учет специфических особенностей силовых структур, не поддающихся формализации; гибкость при отсутствии стандартизированных данных	Субъективность экспертных суждений; высокие временные затраты на проведение оценки; сложность межведомственного сравнения результатов; низкая воспроизводимость и верифицируемость результатов; зависимость от доступности и компетентности экспертов

Анализ выявил ряд системных недостатков, характерных для большинства рассмотренных подходов. Во-первых, недостаточный учет специфики деятельности силовых структур, включая режим секретности, жесткую иерархию и приоритет боеготовности над эффективностью в обычном понимании. Во-вторых, слабость механизмов интеграции технических метрик с показателями оперативной эффективности. В-третьих, недостаточное внимание к оценке деятельности ИТ-подразделений в условиях активного противодействия, в частности в условиях радиоэлектронного подавления, кибератак и физического уничтожения инфраструктуры. В-четвертых, ограниченность большинства подходов стратегическим или тактическим уровнем при недостаточном внимании к оперативному уровню военного управления.

Заключение

Проведенный систематический обзор существующих подходов к оценке деятельности ИТ-подразделений информационных технологий силовых структур позволяет сформулировать следующие основные выводы.

Деятельность ИТ-подразделений силовых структур носит дуальный характер, сочетая в себе функции классического ИТ-департамента государственного органа и высокоспециализированного оператора защищенных систем связи военного назначения. Ни один из существующих подходов в отдельности не способен обеспечить всестороннюю оценку эффективности их работы. Каждый из рассмотренных подходов обладает собственными достоинствами и ограничениями применительно к условиям деятельности силовых структур.

Наиболее существенными ограничениями является слабость механизмов связи технологических показателей с оперативными результатами на всех уровнях управления, недостаточность инструментария оценки деятельности в условиях активного противодействия, а также ограниченность внимания к специфике систем связи как критического элемента военной инфраструктуры.

Теоретическая и практическая значимость исследования состоит в следующем. В теоретическом плане результаты исследования формируют систематизированную научную основу для дальнейших разработок в области методического обеспечения оценки деятельности ИТ-подразделений силовых структур. В практическом плане выявленные достоинства и ограничения существующих подходов могут быть использованы при разработке ведомственных методических документов, регламентирующих порядок оценки деятельности ИТ-подразделений, а также при проектировании автоматизированных систем мониторинга деятельности таких подразделений.

Проведенное исследование позволяет определить следующее перспективное направление дальнейших научных разработок, заключающееся в разработке комплексной модели оценки деятельности ИТ-подразделений силовых структур, интегрирующей технологические метрики с показателями оперативной эффективности на всех уровнях управления.

Список литературы

1. *Alberts D.S., Hayes R.E.* Power to the edge: Command... control... in the information age. – 2003.
2. *Sproles N.* Establishing measures of effectiveness for command and control: A systems engineering perspective. – 2001. – №. DSTOGD0278.
3. *Davis L.M., Jackson B.A.* Evaluating Information Technology // Information technology and the criminal justice system. – 2005. – P. 29.
4. *Исаев О.В.* Разработка моделей и алгоритмов анализа эффективности информационных структур и процессов охранных систем: диссертация на соискание ученой степени кандидата технических наук, 2014. – 177 с. – EDN KRQMUN.
5. *Грачева Е.А., Поначугин А.В.* Оценка эффективности работы ИТ-отдела // Экономика. Информатика. – 2022. – Т. 49, № 1. – С. 153-158. – DOI 10.52575/2687-0932-2022-49-1-153-158. – EDN PJEPUI.
6. *Ernawati Y., Wang G.* Assessing IT services management with ITIL framework V3: A case study // Journal of System and Management Sciences. – 2023. – V. 13. – No. 4. – P. 152-164. – DOI :10.33168/JSMS.2023.0409
7. *Mosweu O.E.* An assessment of the capacity management process of the information technology infrastructure library (ITIL) framework in delivering value in public sector. – Cape Peninsula University of Technology, 2017. – URL: http://hdl.handle.net/20.500.11838/2662
8. *Hanafi R., Wibowo L. A., Rahayu A.* Organization and IT strategic alignment, determination of IT process priorities using COBIT 5 // 2020 International Conference on Advancement in Data Science, E-learning and Information Systems (ICADEIS). – IEEE, 2020. – С. 1-6. – DOI 10.1109/ICADEIS49811.2020.9277302
9. *Essien I.A. et al.* Optimizing cyber risk governance using global frameworks: ISO, NIST, and COBIT alignment // Journal of Frontiers in Multidisciplinary Research. – 2022. – V. 3. – No 1. – P. 618-629. – DOI 10.54660/.JFMR.2022.3.1.618-629
10. *Исаев Е.А., Коровкина Н.Л., Табакова М.С.* Оценка готовности ИТ-подразделения компании к цифровой трансформации бизнеса // Бизнес-информатика. – 2018. – № 2(44). – С. 55-64. – EDN UTSMPG.
11. *Becker J., Knackstedt R., Pöppelbuß J.* Developing maturity models for IT management: A procedure model and its application // Business & information systems engineering. – 2009. – V. 1. – No. 3. – С. 213-222.
12. Chrissis M.B., Konrad M., Shrum S. CMMI for development: guidelines for process integration and product improvement. – Pearson Education, 2011.
13. *de Sousa Pereira R.F., Da Silva M.M.* A maturity model for implementing ITIL v3 // 2010 6th World Congress on Services. – IEEE, 2010. – P. 399-406. – DOI 10.1109/SERVICES.2010.80
14. *Ernawati Y., Wang G.* Assessing IT services management with ITIL framework V3: A case study // Journal of System and Management Sciences. – 2023. – V. 13. – No. 4. – P. 152-164. – DOI 10.33168/JSMS.2023.0409
15. *Alberts D.S., Huber R.K., Moffat J.* NATO NEC C2 maturity model. – 2010.
16. *Bruzzone A. et al.* CGF for NATO NEC C2 maturity model (N2C2M2) evaluation // Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2009. – 2009. – P. 1-9.
17. *Kaplan R.S., Norton D.P.* Linking the balanced scorecard to strategy // California management review. – 1996. – V. 39. – No. 1. – P. 53-79. – DOI 10.2307/41165876
18. *Kaplan R.S.* Conceptual foundations of the balanced scorecard //Handbooks of management accounting research. – 2009. – V. 3. – p. 1253-1269. – DOI 10.1016/S1751-3243(07)03003-9
19. *Ivancík R., Necas P.* System of Balanced Scorecard and its Impelementation in Management of Norwegian Air Force and other Military Organizations // Incas Bulletin. – 2012. – V. 4. – No. 4. – P. 141. – DOI 10.13111/2066-8201.2012.4.4.13
20. United States Department of Defense. DoD Information Technology Standards Registry (DISR). – Washington: DoD CIO, 2021. — URL: https://itlaw.fandom.com/wiki/DoD_Information_Technology_Standards_and_Profile_Registry (дата обращения: 15.10.2025).

21. *Carmona S., Grönlund A.* Measures vs actions: the balanced scorecard in Swedish Law Enforcement // International Journal of Operations & Production Management. – 2003. – V. 23. – No. 12. – P. 1475-1496. – DOI 10.1108/01443570310506722

22. *Northcott D., Ma'amora Taulapapa T.* Using the balanced scorecard to manage performance in public sector organizations: Issues and challenges // International Journal of Public sector management. – 2012. – V. 25. – No. 3. – P. 166-191. – DOI 10.1108/09513551211224234

23. *Parmenter D.* Key performance indicators: developing, implementing, and using winning KPIs. – John Wiley & Sons, 2015.

24. *Vitus O.V., Iliashenko O.Yu.* Definition and monitoring KPI for the local it Department / O. V. Vitus, // Неделя науки СПбПУ: Материалы научной конференции с международным участием. Институт промышленного менеджмента, экономики и торговли. В 3-х частях, Санкт-Петербург, 18–23 ноября 2019 года. Vol. Часть 1. – СПб: Санкт-Петербургский политехнический университет Петра Великого, 2019. – С. 15-19. – EDN DMVLPQ.

25. *Weaver J.M.* NATO Communications & Information Systems Group (NCISG) // NATO in Contemporary Times: Purpose, Relevance, Future. – Cham: Springer International Publishing, 2021. – P. 123-136. – DOI 10.1007/978-3-030-68731-1_10

26. *Folorunso A. et al.* The impact of ISO security standards on enhancing cybersecurity posture in organizations // World Journal of Advanced Research and Reviews. – 2024. – V. 24. – No. 1. – P. 2582-2595. – DOI 10.30574/wjarr.2024.24.1.3169

27. *Boyes H., Higgins M.D.* An overview of information and cyber security standards // Journal of ICT Standardization. – 2024. – V. 12. – No. 1. – P. 95-134. DOI 10.13052/jicts2245-800X.1215

28. *Martins J. et al.* Information Security–Military Standards Versus ISO 27001: A Case Study in a Portuguese Military Organization // Information Warfare and Security. – 2013. – P. 191.

29. *Mulazzani F., Sarcia S. A.* Cyber security on military deployed networks // 2011 3rd International Conference on Cyber Conflict. – IEEE, 2011. – P. 1-15.

30. *Бурянин С.Н.* Методика оценки эффективности подразделений связи и радиотехнического обеспечения полетов авиации Воздушно-космических сил // Системы управления, связи и безопасности. – 2020. – № 4. – С. 220-239. – DOI 10.24411/2410-9916-2020-10408. – EDN EBRJSH.

Статья поступила в редакцию 14 сентября 2025 г.
Принята к публикации 24 декабря 2025 г.

Ссылка для цитирования: Аскеров Р.А. Анализ подходов к оценке деятельности подразделений информационных технологий и связи силовых структур // Национальная безопасность и стратегическое планирование. 2025. № 4(52). С. 18-28. DOI: https://doi.org/10.37468/2307-1400-2025-4-18-28

Analysis of approaches to assessing the activities of information technology and communications units of law enforcement agencies

***Askerov Roman A.*[1]**

[1] *Main Directorate of the Ministry of Emergency Situations of Russia for the Khanty-Mansi Autonomous Okrug - Yugra, Khanty-Mansiysk, Russia*

Abstract

The relevance of this study is determined by the increasing dependence of law enforcement agencies on information and telecommunications systems and the need for objective monitoring of the effectiveness of information technology and communications units. The objective of the study is to comparatively analyze existing approaches to assessing the performance of information technology and communications units of law enforcement agencies, identifying their advantages, limitations, and prospects for adaptation to the specifics of law enforcement agencies. The article presents a typology of approaches, including basic IT service management methodologies (ITIL, COBIT), IT process maturity models, key performance indicator (KPI) systems, specialized standards, and expert assessment methods. Common shortcomings of existing approaches are identified (weak connection between technological metrics and operational results, insufficient consideration of active counteraction conditions). The significance of

the study lies in the formation of a systematized scientific basis for further developments in the field of methodological support for assessing the performance of IT units of law enforcement agencies. The practical significance lies in the possibility of using the identified advantages and disadvantages of the analyzed approaches in the development of departmental methodological documents and automated systems for monitoring the activities of IT units. Prospects for further research are related to the development of a comprehensive model for assessing the performance of IT departments of law enforcement agencies, integrating technological metrics with operational performance indicators at all levels of management.

Keywords: performance evaluation, information technology, communications, law enforcement agencies, key performance indicators, IT departments, evaluation methods.

References

1. *Alberts D.S., Hayes R.E.* Power to the edge: Command... control... in the information age. – 2003.
2. *Sproles N.* Establishing measures of effectiveness for command and control: A systems engineering perspective. – 2001. – №. DSTOGD0278.
3. *Davis L.M., Jackson B.A.* Evaluating Information Technology // Information technology and the criminal justice system. – 2005. – P. 29.
4. *Isaev O.V.* Development of models and algorithms for analyzing the effectiveness of information structures and processes of security systems: dissertation for the degree of candidate of technical sciences, 2014. – 177 p. – EDN KRQMUN.
5. *Gracheva E.A., Ponachugin A.V.* Evaluation of the effectiveness of the IT department // Economics. Informatics. – 2022. – Vol. 49, No. 1. – Pp. 153-158. – DOI 10.52575/2687-0932-2022-49-1-153-158. – EDN PJEPUI.
6. *Ernawati Y., Wang G.* Assessing IT services management with ITIL framework V3: A case study // Journal of System and Management Sciences. – 2023. – V. 13. – No. 4. – P. 152-164. – DOI :10.33168/JSMS.2023.0409
7. *Mosweu O. E.* An assessment of the capacity management process of the information technology infrastructure library (ITIL) framework in delivering value in public sector. – Cape Peninsula University of Technology, 2017. – URL: http://hdl.handle.net/20.500.11838/2662
8. *Hanafi R., Wibowo L.A., Rahayu A.* Organization and IT strategic alignment, determination of IT process priorities using COBIT 5 // 2020 International Conference on Advancement in Data Science, E-learning and Information Systems (ICADEIS). – IEEE, 2020. – C. 1-6. – DOI 10.1109/ICADEIS49811.2020.9277302
9. *Essien I.A. et al.* Optimizing cyber risk governance using global frameworks: ISO, NIST, and COBIT alignment // Journal of Frontiers in Multidisciplinary Research. – 2022. – V. 3. – No 1. – P. 618-629. – DOI 10.54660/.JFMR.2022.3.1.618-629
10. *Исаев Е.А., Коровкина Н.Л., Табакова М.С.* Оценка готовности ИТ-подразделения компании к цифровой трансформации бизнеса // Бизнес-информатика. – 2018. – № 2(44). – С. 55-64. – EDN UTSMPG.
11. *Becker J., Knackstedt R., Pöppelbuß J.* Developing maturity models for IT management: A procedure model and its application // Business & information systems engineering. – 2009. – V. 1. – No. 3. – C. 213-222.
12. *Chrissis M. B., Konrad M., Shrum S.* CMMI for development: guidelines for process integration and product improvement. – Pearson Education, 2011.
13. *de Sousa Pereira R.F., Da Silva M.M.* A maturity model for implementing ITIL v3 // 2010 6th World Congress on Services. – IEEE, 2010. – P. 399-406. – DOI 10.1109/SERVICES.2010.80
14. *Ernawati Y., Wang G.* Assessing IT services management with ITIL framework V3: A case study // Journal of System and Management Sciences. – 2023. – V. 13. – No. 4. – P. 152-164. – DOI 10.33168/JSMS.2023.0409
15. *Alberts D.S., Huber R.K., Moffat J.* NATO NEC C2 maturity model. – 2010.
16. *Bruzzone A. et al.* CGF for NATO NEC C2 maturity model (N2C2M2) evaluation // Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2009. – 2009. – P. 1-9.
17. *Kaplan R. S., Norton D. P.* Linking the balanced scorecard to strategy // California management review. – 1996. – V. 39. – No. 1. – P. 53-79. – DOI 10.2307/41165876
18. *Kaplan R.S.* Conceptual foundations of the balanced scorecard //Handbooks of management accounting research. – 2009. – V. 3. – p. 1253-1269. – DOI 10.1016/S1751-3243(07)03003-9
19. *Ivancík R., Necas P.* System of Balanced Scorecard and its Impelementation in Management of Norwegian Air Force and other Military Organizations // Incas Bulletin. – 2012. – V. 4. – No. 4. – P. 141. – DOI 10.13111/2066-8201.2012.4.4.13

20. United States Department of Defense. DoD Information Technology Standards Registry (DISR). – Washington: DoD CIO, 2021. — URL: https://itlaw.fandom.com/wiki/DoD_Information_Technology_Standards_and_Profile_Registry (дата обращения: 15.10.2025).

21. *Carmona S., Grönlund A.* Measures vs actions: the balanced scorecard in Swedish Law Enforcement // International Journal of Operations & Production Management. – 2003. – V. 23. – No. 12. – P. 1475-1496. – DOI 10.1108/01443570310506722

22. *Northcott D., Ma'amora Taulapapa T.* Using the balanced scorecard to manage performance in public sector organizations: Issues and challenges // International Journal of Public sector management. – 2012. – V. 25. – No. 3. – P. 166-191. – DOI 10.1108/09513551211224234

23. *Parmenter D.* Key performance indicators: developing, implementing, and using winning KPIs. – John Wiley & Sons, 2015.

24. *Vitus O.V., Iliashenko O.Yu.* Definition and monitoring KPI for the local IT Department / O. V. Vitus, // SPbPU Science Week: Proceedings of the scientific conference with international participation. Institute of Industrial Management, Economics and Trade. In 3 parts, St. Petersburg, November 18–23, 2019. Vol. Part 1. – SPb: Peter the Great St. Petersburg Polytechnic University, 2019. – P. 15–19. – EDN DMVLPQ.

25. *Weaver J.M.* NATO Communications & Information Systems Group (NCISG) // NATO in Contemporary Times: Purpose, Relevance, Future. – Cham: Springer International Publishing, 2021. – P. 123-136. – DOI 10.1007/978-3-030-68731-1_10

26. *Folorunso A. et al.* The impact of ISO security standards on enhancing cybersecurity posture in organizations // World Journal of Advanced Research and Reviews. – 2024. – V. 24. – No. 1. – P. 2582-2595. – DOI 10.30574/wjarr.2024.24.1.3169

27. *Boyes H., Higgins M. D.* An overview of information and cyber security standards // Journal of ICT Standardization. – 2024. – V. 12. – No. 1. – P. 95-134. DOI 10.13052/jicts2245-800X.1215

28. *Martins J. et al.* Information Security–Military Standards Versus ISO 27001: A Case Study in a Portuguese Military Organization // Information Warfare and Security. – 2013. – P. 191.

29. *Mulazzani F., Sarcia S.A.* Cyber security on military deployed networks // 2011 3rd International Conference on Cyber Conflict. – IEEE, 2011. – P. 1-15.

30. *Buryanin S.N.* Methodology for assessing the effectiveness of communications units and radio technical support for flights of aviation of the Aerospace Forces // Control, Communications and Security Systems. – 2020. – No. 4. – P. 220-239. – DOI 10.24411/2410-9916-2020-10408. – EDN EBRJSH.

For citation: Askerov R.A. Analysis of approaches to assessing the activities of information technology and communications units of law enforcement agencies // National security and strategic planning. 2025. № 4(52). pp. 18-28. DOI: https://doi.org/10.37468/2307-1400-2025-4-18-28

Информация об авторах:

Аскеров Роман Айвазович – Главное управление МЧС России по Ханты-Мансийскому автономному округу - Югре, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, г. Ханты-Мансийск, Россия
SPIN-код: 9099-8858
e-mail: rask05@yandex.ru

Information about authors:

Askerov Roman A. – Main Directorate of the Ministry of Emergency Situations of Russia for the Khanty-Mansi Autonomous Okrug - Yugra, Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters, Khanty-Mansiysk, Russia
SPIN-код: 9099-8858
e-mail: rask05@yandex.ru