МНОГОУРОВНЕВЫЙ ФРЕЙМВОРК ОБОСНОВАНИЯ ПРОЦЕДУР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Грызунов В. В.[1], Шестаков А. В.[2]

DOI: 10.21681/2311-3456-2025-6-14-24

Цель исследования: *обосновать подходы к рациональной организации мониторинга и реагирования на возможные инциденты информационной безопасности.*

Метод исследования: *информационная система описывается разработанной и апробированной авторами иерархической моделью, включающей обеспечивающий уровень, уровень персонала, а также уровни аппаратного и программного обеспечения. Модель получает на вход множества возможных состояний информационной системы и инцидентов информационной безопасности, допустимые значения вероятностей рисков информационной безопасности и множество допустимых управляющих воздействий. На выходе модели – управляющее воздействие, которое удерживает вероятность риска информационной безопасности в заданном диапазоне.*

Полученный результат: *многоуровневый фреймворк обеспечивает сквозное описание процесса управления инцидентами информационной безопасности — от обнаружения инцидента до формирования плана улучшений. Он позволяет количественно оценивать эффективность мер реагирования на каждом уровне информационной системы – обеспечивающем, персонала, аппаратном и программном. Ключевое преимущество подхода – возможность компенсировать недостатки одного уровня за счёт усиления другого, что расширяет возможности удержать вероятность риска информационной безопасности в заданном диапазоне. На основе полученных оценок формируются экономически обоснованные стратегии информационной безопасности. Центральным практическим выводом является принцип «перераспределения риска», который заменяет догматическое требование устранить все уязвимости на целенаправленное, измеримое и рентабельное управление вероятностью риска.*

Научная новизна: *в отличие от существующих моделей разработанная модель явно учитывает совокупную вероятность риска информационной безопасности и взаимозависимость всех четырёх уровней информационной системы за счёт формирования соответствующего оператора.*

Ключевые слова: *терминосистема, кибербезопасность, управление инцидентами.*

Введение

Процессы мониторинга инцидентов информационной безопасности (ИИБ) и реагирования на ИИБ вынужденно входят в повседневную деятельность компаний, - к этому побуждает и законодательство, и экономические соображения. Результаты анализа нормативных правовых актов (НПА), в части необходимости мониторинга и реагирования на ИИБ, подтверждают несогласованность периодичности мониторинга и реагирования (табл. 1).

Анализ доступной статистики об утечках персональных данных подтверждает экономическими показателями положительный эффект регламентированного тестирования ИС, а регулярного мониторинга угроз ИБ с применением SIEM (Security Information and Event Management), MDR (Managed Detection and Response) и CEM (Continuous Exposure Management) – вероятностными показателями. Средства мониторинга и реагирования на ИИБ

Таблица 1.

Сводные данные из НПА в части мониторинга и реагирования на ИИБ

Документ	Мониторинг / Обнаружение	Регистрация / Отчёт	Реагирование (сроки)
ГОСТ Р 59547 / Р 59709	да	да	да
ГОСТ ИСО/МЭК ТО 18044 2007	Не определено	Немедленно	По итогам формы отчёта
Приказ ФСБ № 282 (КИИ)	Сенсоры / круглосуточно	В течение 3 ч / 24 ч	В течение 48 ч
Положение ЦБ № 822 П (страхование)	Регистрация событий	Описание мер	В сроки регулятора

1 Грызунов Виталий Владимирович, доктор технических наук, доцент, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России. Санкт-Петербург, Россия. ORCID https://orcid.org/0000-0003-4866-217X. E-mail: viv1313r@mail.ru

2 Шестаков Александр Викторович, доктор технических наук, старший научный сотрудник, ведущий научный сотрудник Санкт-Петербургского университета ГПС МЧС России. Санкт-Петербург, Россия. ORCID https://orcid.org/0000-0002-8462-6515. E-mail: alexandr.shestakov01@yandex.ru

Таблица 2.

Сущности мониторинга и реагирования на возможные ИИБ в НПА

Элемент стандарта	Мониторинг / обнаружение	Реагирование / ответ
ГОСТ 57580.1	Мониторинг событий ИБ и их регистрация	Классификация и организация реакции
ГОСТ 57580.3/4	Мониторинг рисков и событий	Реакция и восстановление после инцидентов
NIST 800 61r3	Фаза Detection & Analysis (SIEM, IDS)	Фаза Response & Recovery
ISO 27035	Обнаружение и оценка событий и инцидентов	Реакция, восстановление, анализ уроков

становятся неотъемлемой частью системы управления ИИБ.

Анализ руководящих документов подтверждает, что мониторинг и реагирование на ИИБ являются частью процесса управления ИИБ (табл. 2).

Цель настоящего исследования – обосновать подходы к рациональной организации мониторинга и реагирования на возможные ИИБ.

Анализ литературы

Формализованный подход к автоматизации обнаружения и реагирования на инциденты ИБ изложен в статье [1]. Основу составляют система поддержки принятия решений (СППР) с моделью на базе теории графов и нечеткой логики, которая соотносит наблюдаемые события с типами инцидентов. Не в полной мере учтён человеческий фактор и множество допустимых состояний системы, которое определено руководящими документами. Модель предполагает наличие оператора, но не рассматривает вопросы его подготовки, квалификации или действий в нештатных ситуациях. Отсутствует анализ возможности интеграции предложенного плана в существующую нормативную базу организации, например, в планы обеспечения непрерывности деятельности.

Комплексный подход к созданию Центра мониторинга ИБ (SOC) предложен в [2]. Описана процессная модель по рекомендациям NIST, структура команды (три линии поддержки). Программно-аппаратная среда рассматривается упрощенно, без учета сложностей гетерогенных инфраструктур (гибридные облака, АСУ ТП) и возможности отказа самих средств мониторинга. Отсутствует описание влияние уровней SOC друг на друга.

Прогрессивная концепция управления ИБ на основе цикла непрерывного детектирования и реагирования (CD/CR), аналогичного DevOps-подходу CI/CD изложена в [3]. Фокус смещается с физической инфраструктуры на абстрактный «управляемый объект», а сценарии реагирования (playbooks) формируются динамически на основе обогащенного контекста инцидента, что позволяет адаптироваться к меняющимся угрозам и проводить глубокий контекстно-ориентированный анализ атак. Концепция строится на идеализированном предположении о полноте и достоверности собираемых данных, не учитывая «туман войны»: сбои средств мониторинга, нелогируемые техники атак и другие проблемы. Человеческий фактор не учитывается.

Подход к формализации процесса обнаружения инцидентов ИБ на промышленных предприятиях рассмотрен в [4]. Исследование фокусируется на выработке общего математического критерия, представляя мониторинг как вероятностный процесс. На основе теории случайных процессов проанализировано, как различные факторы (сбои оборудования, ошибки ПО, действия персонала) вносят погрешность в измерения и влияют на итоговую вероятность обнаружения. Программно-аппаратная среда рассматривается абстрактно, как источник статистического «шума», без учета всех ее состояний, таких как «полный отказ средств мониторинга».

В контексте «умных городов» рассмотрена проблематика кибербезопасности [5]. Приведён комплексный и актуальный охват темы, затрагивающий технические, организационные и правовые вопросы, однако не содержит детальных технических решений, не формализует связь программно-аппаратного комплекса, персонала и руководящих документов.

Интегрированная система управления киберрисками (i-CSRM) в [6] основана на модели, которая объединяет данные о киберугрозах (CTI), оценку критичности активов с помощью нечёткой логики, прогнозирование рисков на основе машинного обучения и проверку эффективности уже внедрённых средств защиты. Процессы мониторинга и реагирования выступают элементом модели и являются несколько статичными. При этом модель опирается на существующие навыки персонала. Не описано, как модель вписывается во внутренние регламенты организации.

В работе [7] авторы описывают процессы мониторинга и реагирования на ИИБ средствами облачного центра мониторинга (SOC) в Microsoft Azure, в которой развёрнута защищённая виртуальная

сеть (VNet) с межсетевым экраном для веб-приложений (WAF). Инфраструктура интегрирована с SIEM-системой Microsoft Sentinel для мониторинга событий и с Microsoft Defender for Cloud для контроля безопасности и соответствия. Реакция системы тестируется с помощью nmap. Для персонала сделан акцент на модели разделения ответственности между потребителем облака и поставщиком облачных услуг. Работа опирается на фреймворки NIST, CSA и Azure Well-Architected Framework. Реализованное решение позволяет проводить автоматическую оценку на соответствие стандартам GDPR, PCI-DSS, ISO 27001, а конфигурация WAF основана на правилах OWASP.

Экономико-математический подход для обоснования формирования бюджета на ИБ, реализованный на Python, описан в [8]. Программа моделирует состояние бюджета на ИБ, из которого покрываются случайные расходы на устранение инцидентов. В основе лежат положения теории рисков и математики страхования.

Методы исследования

Информационная система (ИС) в настоящем исследовании рассматривается как комплексная организационно-техническая система, имеющая несколько иерархических уровней. Поэтому для её описания целесообразно использовать разработанную и апробированную авторами иерархическую модель информационной системы, включающая обеспечивающий уровень, уровень персонала, а также уровни аппаратного и программного обеспечения.

Метауровни задают требуемые состояния (S) вложенных уровней. Обеспечивающий уровень имеет множество (S^E) состояний, формирует требования к персоналу (П) и к программно-аппаратному комплексу, то есть задаёт требования к множествам состояний (S^P) уровня персонала, уровня (S^{Hard}) аппаратного обеспечения (АО) и уровня (S^{Soft}) программного обеспечения (ПО). Персонал настраивает и обеспечивает функционирование аппаратного и программного обеспечения, то есть задаёт требования к множествам S^{Hard} и S^{Soft}. Аппаратура, в свою очередь, предоставляет заданные ресурсы и среду исполнения для ПО, то есть задаёт требования к S^{Soft}. Например, ПО функционирует в рамках системы команд и ограничений доступа к памяти, заданных аппаратной платформой, а аппаратура эксплуатируется персоналом в соответствии с установленными регламентами.

Примеры состояний каждого уровня ИС

Обеспечивающий уровень – объём финансирования в месяц (s_1^E), требования по повышению квалификации персонала (s_2^E), требование ко времени предоставления отчётов об ИББ (s_3^E).

Уровень персонала – компетенции персонала в сфере ИБ (s_1^P), загрузка в течение рабочего дня (s_2^P), укомплектованность специалистами ИБ (s_3^P).

Уровень АО – наличие резервного канала связи (s_1^{Hard}), включение устройства защиты от ПЭМИН (s_2^{Hard}), применение внешнего сервера для сбора данных от DLP-агентов (s_3^{Hard}).

Уровень ПО – развёрнута SIEM-система (s_1^{Soft}), установлено антивирусное ПО (s_2^{Soft}), применение TLS (s_3^{Soft}).

Декартово произведение состояний каждого уровня формирует общее состояние ИС (S)

$$S = S^E \times S^P \times S^{Hard} \times S^{Soft}. \quad (1)$$

Вложенный уровень влияет на метауровень через обратную связь. Например, выявление ограничения на уровне ПО, не позволяющего организовать работу распределённой в пространстве-времени команды специалистов ИБ, может потребовать распределить работу в пространстве-времени АО. Что, в свою очередь, откорректирует требования к квалификации персонала и инициирует изменения регламентов или финансирования на обеспечивающем уровне.

В настоящем исследовании используется модель системы адаптивного управления на базе операторного уравнения, разработанная авторами в интересах киберполигона МЧС России.

Результаты

Анализ НПА в сфере ИБ подтверждает, что одна из главных целей управления ИИБ – своевременное реагирование для ограничения ущерба (снижения риска ИИБ). Соответственно, процессы мониторинга и реагирования как часть системы управления ИИБ, во-первых, должны работать на эту же цель – снизить риск ИБ, во-вторых, должны быть согласованы между собой.

Риск ИБ (Ψ_a), ущерб (W) и вероятность риска ИБ (P_{risk}) могут рассчитываться таблично, посредством лингвистических переменных (критический, высокий, низкий и т.п.) или аналитически. Существует ряд способов свести к аналитическому виду представление величин в виде лингвистической переменной. Например, для вероятности риска для каждого значения лингвистической переменной определяются границы значения вероятности риска: низкий [0; 0,2), средний [0,2; 0,4), высокий [0,4; 1]. Затем вместо каждого значения лингвистической переменной подставляется среднее значение соответствующего интервала. Поэтому далее без нарушения общности и для повышения наглядности воспользуемся аналитическим способом расчёта риска ИБ:

$$\Psi_a = P_{risk}\, W. \quad (2)$$

Обычно специалисты ИБ не влияют на ущерб, возникающий в ходе возникновения ИИБ, потому

что ущерб определяется целевыми процессами ИС. Специалисты ИБ снижают вероятность риска ИБ (P_{risk}).

Риск ИБ – это мера опасности ИБ, а мера безопасности ИС – доверие, как показано в [9]. При этом термин «доверие» в различных источниках применяется без его точного определения, либо приводятся определения в стиле «доверие – это основания для обоснованной уверенности в том, что объект оценки соответствует функциональным требованиям безопасности», которые не дают представления об единицах измерения «доверия», и следовательно, не позволяют измерить «доверие». Примем в состав терминосистемы настоящего исследования следующие определения.

Определение. Доверие – это величина, дополняющая вероятность риска ИБ до единицы

$$D = 1 - P_{risk}. \quad (3)$$

Определение. Безопасная ИС (ИС, которой можно доверять) с точки зрения информационной безопасности является та ИС, в которой отсутствуют ИИБ.

В «безопасной ИС», согласно предложенной модели ИС, должно быть «доверие» ко всем уровням ИС. В общем случае, исходя из практического опыта, существует позитивная корреляция между «событиями», состоящими в том, что есть «доверие на уровнях ИС». Если есть «доверие» на уровне персонала, то вероятность того, что будет «доверие» на других уровнях (АО или ПО, обеспечивающего уровня) увеличивается. Или выделение финансирования (обеспечивающий уровень) повышает вероятность закупки и своевременного обновления программ и оборудования (ПО и АО), финансовой мотивации персонала (уровень персонала).

Пусть x^i – событие, означающее «на уровне i можно доверять» (отсутствует инцидент). Тогда $P(x^i) = D^i$.

Совокупное доверие — это вероятность того, что всем уровням можно доверять одновременно: $D = P(x^E \cap x^P \cap x^{Hard} \cap x^{Soft})$.

Если события x^i положительно коррелированы, то по определению $P(A \cap B) \geq P(A)P(B)$. Распространяя это на n событий, получаем:

$$P(x^i) \geq \prod P(x^i). \quad (4)$$

Следовательно, произведение вероятностей действительно является нижней границей, и если принять в качестве ограничения независимость событий, состоящих в существовании доверия на каждом уровне, то мы получим нижнюю оценку доверия ко всей ИС, что оправдано с точки зрения обеспечения ИБ. Нижняя граница доверия ко всей ИС будет вычисляться по формуле:

$$D = D^E \times D^P \times D^{Hard} \times D^{Soft}. \quad (5)$$

Из (4) следует, что вероятность общего риска ИБ будет равна:

$$P_{risk} = 1 - D = 1 - (1 - P^E_{risk})(1 - P^P_{risk}) \times \times (1 - P^{Hard}_{risk})(1 - P^{Soft}_{risk}). \quad (6)$$

Выражение (5) даёт нам верхнюю оценку вероятности общего риска ИБ.

Из (5) следует, что вероятность общего риска ИБ ИС (далее вероятность риска) может быть снижена специалистами ИБ на каждом уровне ИС.

Множество возможных ИИБ в ИС (Q) включает в себя ИИБ для каждого уровня ИС:

Обеспечивающий уровень (Q^E). Урезали финансирование для обновления средств защиты информации (СЗИ), политика ИБ не предусматривает проверку качества резервных копий, отсутствует перечень конфиденциальной информации.

Уровень персонала (Q^P). Не пройдено повышение квалификации персонала на объекте КИИ в течение четырёх лет, пароль администратора известен рядовому пользователю, персонал не осведомлён о том, что опасно «кликать котиков» в электронных письмах.

Уровень аппаратного обеспечения (Q^{Hard}). Активирована закладка в процессоре, вышло из строя устройство защиты от ПЭМИН, выдана недокументированная команда на маршрутизатор.

Уровень программного обеспечения (Q^{Soft}). Распространение шифровальщика, реализовано повышение привилегий учётной записи пользователя, выполнена атака Tiny Fragment Attack.

$$Q = Q^E \times Q^P \times Q^{Hard} \times Q^{Soft}. \quad (7)$$

Управлять ИИБ, исходя из состояния ИС, означает сделать выбор управляющего воздействия из множества ($U_{доп}$) допустимых управляющих воздействий на основе множеств ИИБ и состояний ИС в каждый момент времени (T) функционирования ИС. Другими словами, для каждой комбинации возникших инцидентов, состояний системы и моментов времени существует предписанное управляющее воздействие. Существует множество отображений (A) булеана (B) во множество допустимых управляющих воздействий для каждого уровня ИС:

$$B^{ИС} = \begin{cases} B^E \cup B^P \cup B^{Hard} \cup B^{Soft} \\ B^E = B(S^E \cup Q^E \cup T) \\ B^P = B(S^P \cup Q^P \cup T) \\ B^{Hard} = B(S^{Hard} \cup Q^{Hard} \cup T) \\ B^{Soft} = B(S^{Soft} \cup Q^{Soft} \cup T) \end{cases}, \quad (8)$$

$$A = A^E \times A^P \times A^{Hard} \times A^{Soft}: \begin{cases} B^E \xrightarrow{A^E} U^E \\ B^P \xrightarrow{A^P} U^P \\ B^{Hard} \xrightarrow{A^{Hard}} U^{Hard} \\ B^{Soft} \xrightarrow{A^{Soft}} U^{Soft} \end{cases}. \quad (9)$$

Фактически, множество A содержит субстанциальные закономерности (существенные для достижения цели деятельности ИС [10]), которые описывают процессы в ИС (закрыли порт на межсетевом экране – трафик не идет, сократили бюджет на выплату денежного содержания специалистов – отток кадров). Субстанциальные закономерности могут быть представлены аналитически, статистически, табличо и т.д.

Один из вариантов представления элемента множества допустимых управляющих воздействий $u \in U_{\text{доп}}$ – кортеж с названием действия (u_n) и снижением вероятности риска (Δp):

$$u_i = \langle u_n, \Delta p \rangle_{i \in U}. \quad (10)$$

С одной стороны, включение защитных мер иногда ограничивает выполнение защищаемых бизнес-процессов. С другой стороны, если ограничено выполнение бизнес-процессов, значит нарушен аспект информационной безопасности «доступность». Поэтому формирование интегральной характеристики «снижение вероятности риска» является отдельной задачей и выходит за рамки данного исследования. Полагается, что снижение вероятности риска учитывает влияние на бизнес-процессы компании.

Сопоставление каждому допустимому действию конкретной величины вероятности риска выполняется, например, с помощью метода iSOFT [10], который предполагает на основе морфологического ящика последовательный поиск субстанциальных закономерностей, связывающих величины между собой.

По проблематике получения количественной оценки вероятности риска опубликовано значительное количество научных работ. В исследовании [11], рассмотрена UTEM – технико-экономическая модель с повышенной точностью расчета вероятности инцидентов и потерь в IaaS/PaaS/SaaS. Метод MAGIC предложен в [12] для оценки вероятности инцидента на основе анализа «киберпозиции» организации. В работе [13] обоснован упрощенный алгоритм, который сочетает рейтинги риска, защитных мер и угроз на основе показателей инфраструктуры. Моделирование вероятности и масштаба киберрисков на уровне предприятий с реальными данными из базы операционных убытков с применением статистических методов, в том числе peaks-over-threshold (POT) моделей, copula-моделирования и эмпирического распределения для оценки зависимости между частотой и тяжестью инцидентов, проработано в [14].

Таким образом, проблематика оценки вероятности риска ИБ достаточно хорошо изучены и выходят за рамки данной статьи.

Кортеж (9) может быть дополнен другими показателями: скорость реализации, стоимость реализации, привлекаемые ресурсы и т.д. В этом случае задача становится многокритериальной, и может быть реализована специальным ПО при практическом применении. Многокритериальность добавит в постановку задачи дополнительные ограничения либо может учитываться при формировании множества S, что не влияет на авторский подход и будет учтена в последующем.

Предлагается следующая формулировка задачи управления ИИБ.

Постановка задачи управления ИИБ на основе операторного представления

Дано

$T \ni t$ – множество моментов времени функционирования ИС;

$Q \ni q$ – множество возможных ИИБ;

$S \ni s$ – множество состояний ИС;

P_{risk}^{min} – минимальное допустимое значение вероятности риска;

P_{risk}^{max} – максимальное допустимое значение вероятности риска;

$U_{\text{доп}}$ – множество допустимых действий на каждом уровне ИС;

$A \ni a$ – множество отображений булеана во множество действий на каждом уровне ИС.

Требуется

Найти такое управляющее воздействие, которое при возникновении инцидента ИИБ удержит вероятность риска в заданном диапазоне за заданный интервал времени:

$$\forall b \in B^{\text{ИС}} \ \exists \ u \in U_{\text{доп}}: P_{risk} \in [P_{risk}^{min}; P_{risk}^{max}]. \quad (11)$$

То есть найти оператор, рассчитывающий вероятность риска:

$$R_U(Q,S,A,U_{\text{доп}}) = P_{risk} \in [P_{risk}^{min}; P_{risk}^{max}], \quad (12)$$

где R_U – оператор, отображающий множества Q, S, A, $U_{\text{доп}}$ в интервал [0; 1].

Согласно принципу Беллмана, оператор может быть составлен отдельно для каждого уровня ИС и представлять собой композицию операторов для каждого уровня ИС:

$$R_U = R_U^E(Q^E,S^E,A^E,U_{\text{доп}}^E) \circ R_U^P(Q^p,S^P,A^P,U_{\text{доп}}^P) \circ \circ R_U^{Hard}(Q^{Hard},S^{Hard},A^{Hard},U_{\text{доп}}^{Hard}) \circ \circ R_U^{Soft}(Q^{Soft},S^{Soft},A^{Soft},U_{\text{доп}}^{Soft}). \quad (13)$$

Подставив выражение (5) в выражение (6), и преобразовав в неравенство, получим:

$$P_{risk}^{min} \le 1-(1-P_{risk}^E)(1-P_{risk}^P)(1-P_{risk}^{Hard})(1-P_{risk}^{Soft}) \le P_{risk}^{max}. \quad (14)$$

Это означает, что у специалиста ИБ расширяется выбор доступных вариантов в ходе управления ИИБ, так как появляется возможность:

1) управлять ИИБ на разных уровнях ИС,

2) использовать инструмент обоснования своих действий и затрат на всех уровнях ИС,

3) компенсировать невозможность реагирования на одном уровне ИС реагированием на другом уровне ИС.

Фактически, найденный оператор представляет собой набор playbooks, в которых каждое действие имеет свою оценку эффективности, например, процент снижения вероятности риска.

Поскольку метауровни формируют допустимые состояния вложенных уровней, то применение выражения (6) выполняется последовательно от обеспечивающего уровня к уровню ПО, то есть сначала применяются допустимые действия обеспечивающего уровня, затем П, далее уровня АО и уровня ПО.

Если возможно применение нескольких допустимых действий одновременно, то расчёт нового значения вероятности риска выполняется последовательно для каждого допустимого действия. Поскольку выражения (4) и (5) основаны на операции умножения, которая обладает свойством коммуникативности, то порядок выбора допустимых действий для расчёта новой вероятности риска не имеет значения.

Контрольный пример применения обоснования

Пусть имеет место многоэтапная атака с использованием фишинга с целью кражи данных. Предельно допустимая вероятность риска $P_{risk} \in [0{,}3;0{,}5]$.

Сценарий инцидента (Q):

- начальная компрометация: злоумышленники провели целевую фишинговую рассылку на сотрудников финансового отдела. Один из сотрудников перешел по ссылке и ввел свои учетные данные на поддельной странице входа в корпоративный портал;
- закрепление и разведка: атакующие, используя украденные учетные данные, успешно подключились к корпоративной сети через VPN, не защищенный многофакторной аутентификацией (MFA);
- движение и цель: злоумышленники получил доступ к общему сетевому диску, где хранились финансовые отчеты, и начал готовить их к эксфильтрации (упаковке в архив);
- срабатывание защиты: на этапе эксфильтрации сработала DLP-система, заблокировав передачу архива на внешний облачный сервис (например, ya.ru), и отправила алерт в SIEM.

Задача для специалистов ИБ: инцидент был оперативно локализован (учетная запись скомпрометированного пользователя заблокирована, пароль сброшен, доступ атакующих прерван). Однако теперь перед руководителем ИБ (CISO) стоит задача не просто «закрыть тикет», а представить руководству план действий по снижению вероятности повторения подобных инцидентов и обосновать необходимые ресурсы. Это основное применение разработанного подхода.

Шаг 1. Оценка исходного состояния рисков (до инцидента) CISO, используя модель, оценивает текущий уровень вероятности риска P_{risk} для каждого уровня ИС. Эти оценки не берутся «с потолка», а основываются на данных аудитов, пентестов и здравом смысле.

Обеспечивающий уровень. $P_{risk}^{E} = 0{,}2$. Обоснование: политики ИБ существуют, но формальны. Бюджет на ИБ выделяется по остаточному принципу.

Уровень персонала. $P_{risk}^{P} = 0{,}3$. Обоснование: обучение по кибербезопасности (security awareness) не проводилось два года. Результаты последней симуляции фишинга показали высокий click-rate (30 %).

Уровень АО $P_{risk}^{Hard} = 0{,}1$. Обоснование: с оборудованием в целом все в порядке, но отсутствуют аппаратные токены для MFA.

Уровень ПО. $P_{risk}^{Soft} = 0{,}4$. Обоснование: критически важный фактор: на VPN-шлюзе не включен MFA. DLP-система есть, но настроена в режиме «только мониторинг» для многих правил, чтобы не мешать бизнес-процессам.

Рассчитываем общую вероятность риска по формуле (5):

$$P_{risk} = (1 - (1 - 0{,}2)(1 - 0{,}3)(1 - 0{,}1)(1 - 0{,}4) = 0{,}6976.$$

Общая вероятность риска выходит за пределы допуска, что инцидент и подтвердил.

Шаг 2. Формирование множества допустимых действий ($U_{доп}$) и оценка их эффективности (Δp). CISO вместе с командой формирует набор возможных компенсирующих мер (табл. 3).

Ключевой момент: оценка Δp не является экспертным «гаданием», а привязывается к конкретным метрикам и отраслевым данным.

Шаг 3. Анализ сценариев и принятие решения. Теперь CISO может просчитать несколько стратегий и представить их руководству.

Стратегия 1: «Дешево и быстро» (только организационные меры).

Действия: провести обучение ($\Delta p^{P} = 30$ %), перевести DLP в блокировку ($\Delta p^{Soft} = 40\%$).

Новые значения вероятностей риска:

$$P_{risk}^{P} = 0{,}3(1 - 0{,}3) = 0{,}21,\ P_{risk}^{Soft} = 0{,}4(1 - 0{,}4) = 0{,}24,$$

$$P_{risk} = 1 - (1 - 0{,}2)(1 - 0{,}21)(1 - 0{,}1)(1 - 0{,}24) = 0{,}568.$$

Вывод: вероятность риска снижена, но цель [0,3; 0.5] не достигнута.

Стратегия 2: «Комплексная защита» (внедрение MFA).

Действия: выделить бюджет ($\Delta p^{E} = 5\%$), провести обучение ($\Delta p^{P} = 30\%$), внедрить MFA ($\Delta p^{Soft} = 90\%$).

Таблица 3.

Набор допустимых действий

Уровень	$\langle u_n, \Delta p \rangle$		Обоснование для Δp
	Действие (u_n)	Снижение Δp, %	
Обеспечивающий	Утвердить и выделить бюджет на проект внедрения MFA	5	Действие не снижает риск, но разблокирует возможность технических мер. Эффект проявится через снижение рисков на других уровнях. Оценка вклада 5 % за счет формализации процесса.
Персонал	Провести обязательное обучение и фишинг-симуляцию для фин. отдела	30	По данным Verizon DBIR и собственным тестам, эффективное обучение снижает click-rate в 2-3 раза. Если текущий риск персонала на 50 % обусловлен фишингом, то снижение click-rate на 60 % понизит P^{P}_{risk} на 30 %.
АО	Вариант А: включить MFA для всех VPN-пользователей	90	MFA блокирует >99 % атак, связанных с компрометацией учетных данных. Эффективное действие против этого вектора. Снижает риск до нуля.
ПО	Вариант Б: перевести правила DLP в режим блокировки	40	Не предотвратит вход, но остановит кражу данных. Эффективно для снижения ущерба, но слабо влияет на вероятность успешной атаки. Снижение P^{Soft}_{risk} на 40 %.

Новые значения вероятностей риска:

$$P^{E}_{risk} = 0{,}19,\ P^{E}_{risk} = 0{,}21,\ P^{Soft}_{risk} = 0{,}04.$$

$$P_{risk} = 1 - (1 - 0{,}19)(1 - 0{,}21)(1 - 0{,}1)(1 - 0{,}04) = 0{,}447.$$

Вывод: предложенные меры позволяют снизить вероятность риска до допустимого значения.

Преимущества предложенного подхода для CISO-практик

Язык для общения с бизнесом: вместо «нам нужен MFA, потому что это безопасно», CISO говорит: «Стратегия 1 стоит X условных единиц, и мы остаемся в красной зоне риска. Стратегия 2 стоит Y условных единиц, но она переводит нас в приемлемую желтую зону, снижая вероятность инцидента на Z %. Вот расчеты».

Обоснованность: оценка Δp привязана к измеримым показателям (click-rate, отраслевая статистика), а не к субъективным ощущениям. Защищает от вопроса «А почему вы решили, что это поможет?».

Гибкость: модель показывает, что нет единственного идеального решения. Можно комбинировать менее эффективные, но дешевые меры на разных уровнях, чтобы достичь приемлемой вероятности риска.

Структурированный подход: весь процесс от анализа инцидента до формирования плана улучшений уложен в понятный фреймворк.

Порядок обоснования процедуры мониторинга и реагирования на ИИБ

Этап 1. Оценка исходного состояния («As-Is»)

Определение области моделирования: выбрать критически важный бизнес-процесс или систему для анализа (например, атлас ЧС, корпоративная почта, сегмент АСУ ТП).

Декомпозиция по уровням: описать выбранный процесс в терминах четырех уровневой модели:

- обеспечивающий: «Какие политики, бюджеты, регламенты на нее влияют?»;
- персонал: «Кто работает с процессом (пользователи, администраторы, разработчики)?»;
- аппаратный: «На каком оборудовании она работает (серверы, СХД, сетевое оборудование)?»;
- программный: «Какое ПО используется (ОС, СУБД, прикладное ПО)?».

Оценка текущей вероятности риска (P_{risk}).

Для каждого из четырех уровней оценить текущую вероятность возникновения инцидента (P^{E}_{risk}, P^{P}_{risk}, P^{Hard}_{risk}, P^{Soft}_{risk}).

Что делать на практике: использовать данные аудитов, результаты пентестов, статистику инцидентов, отчеты СЗИ, экспертные оценки, сформировать множества S (текущие состояния) и Q (вероятные инциденты).

Связь с моделью статьи: это начальные значения P_{risk} для выражения (5), как в «Шаге 1» контрольного примера.

Этап 2. Определение целевого состояния («To-Be»)

Установка допустимого уровня риска: совместно с руководством и владельцами критического процесса определить целевой диапазон для совокупной вероятности риска $[P^{min}_{risk}; P^{max}_{risk}]$.

Что делать на практике: перевести технические проценты на язык бизнеса с помощью лингвистических

переменных («зеленая», «желтая», «красная» зоны). Связывать вероятность риска со стоимостью ущерба от ИИБ.

Связь с моделью статьи: это правая часть «операторного уравнения» (6).

Этап 3. Формирование набора инструментов (Playbooks)

Разработка каталога допустимых действий ($U_{доп}$). Для каждого уровня составить список возможных компенсирующих мер.

Что делать на практике: мозговой штурм с командой ИБ и ИТ. Примеры: «внедрить MFA», «провести обучение персонала», «купить новый файрвол», «обновить политику паролей».

Связь с моделью статьи: это формирование множества $U_{доп}$.

Оценка эффективности мер (Δp). Для каждого допустимого действия из каталога оценить, на сколько процентов оно снизит вероятность риска на своем уровне.

Что делаем на практике: самый сложный этап. Использовать отраслевую статистику (например, отчеты Verizon DBIR, которые говорят об эффективности MFA), результаты пилотных проектов, экспертные оценки.

Связь с моделью статьи: это присвоение значений Δp элементам из $U_{доп}$, как в табл. 4 контрольного примера. Сформировать множество отображений A.

Этап 4. Анализ сценариев и принятие решения.

Моделирование стратегий реагирования. Взять типичный или недавний инцидент и просчитать несколько вариантов (стратегий) реагирования, комбинируя меры из каталога допустимых действий.

Что делаем на практике: повторять «Шаг 3» из контрольного примера. Считать новую вероятность риска для «быстрого и дешевого» сценария, для «комплексного и дорогого» и т.д.

Связь с моделью статьи: это практическое решение «операторного уравнения» (6) – поиск такой комбинации действий, которая приводит P_{risk} в целевой диапазон.

Выбор и обоснование оптимальной стратегии. Представить руководству расчеты по разным стратегиям с указанием их стоимости и итогового уровня риска. Принять совместное решение.

Этап 5. Внедрение и контроль (цикл PDCA).

Реализация выбранной стратегии. Внедрить утвержденные меры.

Что делаем на практике: разработать SLAs, обновить инструкции, закупить оборудование, провести тренинги, разработать и утвердить руководящие документы.

Мониторинг и переоценка. Отслеживать ключевые показатели эффективности (KPIs), чтобы проверить, был ли достигнут ожидаемый эффект (Δp). Периодически возвращаться к Этапу 1 и пересматривать оценки P_{risk}, чтобы модель оставалась актуальной. Период пересмотра может входить как параметр допустимого действия, снижающего общую вероятность риска P_{risk}.

Этап 6. Повторить для другого критического бизнес-процесса.

Адекватность предложенного подхода обеспечивается корректностью постановки задачи и использования математического аппарата и проверкой на практике в рамках сегмента киберполигона на базе Санкт-Петербургского университета ГПС МЧС России.

Выводы

Таким образом, предлагаемый подход позволяет интегрировать существующие подходы ко всей системе управления ИИБ и обосновать порядок мониторинга и реагирования на ИИБ.

Фундамент (Baseline): нормативно-правовой подход используется для выполнения обязательных требований регуляторов и закона. Это гигиенический минимум. Используется для формирования множеств T, S, A, $U_{доп}$ и отчасти множества Q, например, когда за основу берётся БДУ ФСТЭК России.

Ядро стратегии: риск-ориентированный подход определяет, куда направить основные усилия и ресурсы сверх базовых требований. Применяется для расчёта значений текущих и допустимых вероятностей риска, формирования множеств Q, A и $U_{доп}$.

Механизм реализации: процессный подход (PDCA) обеспечивает непрерывное управление и улучшение системы ИБ. Применяется для формирования множеств S, A и $U_{доп}$.

Продвинутые уровни: Zero Trust, Cyber Resilience и Threat Intelligence используются зрелыми организациями для построения проактивной и глубоко эшелонированной защиты от сложных современных атак. Применяется для формирования множеств Q, A и $U_{доп}$.

Ключевым практическим выводом модели является принцип «перераспределения риска». Позволяет отойти от догматичного требования устранить все уязвимости, перейти к экономически обоснованному управлению ИИБ.

Модель дает CISO математический инструмент для доказательства того, что инвестиции в усиление одного уровня (например, в security awareness персонала) могут принести гораздо больший «возврат на безопасность» (Return on Security Investment), чем дорогостоящие и порой безрезультатные попытки устранить трудноразрешимую проблему на другом уровне иерархии.

Предлагаемый подход является преимущественно стратегическим инструментом для CISO

и IR-менеджера для анализа, планирования и обоснования инвестиций в ИБ, для формирования playbooks.

Подход может использоваться как инструмент поддержки принятия решения SOC-аналитиком в момент атаки, в реальном масштабе времени оценивая эффективность различных сценариев реагирования, таким образом упрощая и ускоряя выбор допустимых действий SOC-аналитика. В этом случае инструмент должен строиться на playbooks, существующих в компании, и расчёты инструмента будут автоматизированы.

В дальнейших исследованиях предусматривается проработка механизмов гармонизации регламентации мониторинга защищенности информационных ресурсов и реагирования на компьютерные инциденты в информационной инфраструктуре организаций с учетом предложенного подхода.

Статья подготовлена в рамках выполнения НИР «Кибермониторинг» по государственному заданию МЧС России (ЕГИСУ НИОКТР №125031703734-4).

Литература

1. Токарев В.Л. Интеллектуальная поддержка обнаружения инцидентов информационной безопасности / В.Л. Токарев, А.А. Сычугов // Моделирование, оптимизация и информационные технологии. 2023. Т. 11, № 1(40). С. 16-17. DOI 10.26102/2310-6018/2023.40.1.006.
2. Киселев А. А., Практика создания центра мониторинга информационной безопасности / А. А. Киселев, И. В. Коротких, В. В. Шотт // Безопасность цифровых технологий. 2022. Т.11, № 1(40). С.39–51.
3. Олейникова А. А. Концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты безопасности информации / А. А. Олейникова, В. В. Золотарев // Известия ЮФУ. Технические науки. – 2023. – № 5(235). С. 66–81. DOI 10.18522/2311-3103-2023-5-66-81.
4. Гончаренко С. Н., Лачихина А. Б. Мониторинг инцидентов безопасности геоинформационной системы управления и контроля деятельности промышленного предприятия // Горный информационно-аналитический бюллетень (научно-технический журнал). – 2022. – №. 3. С. 108–116
5. Ma, C. Smart city and cyber-security; technologies used, leading challenges and future recommendations // Energy Reports. 2021. Т. 7. С. 7999–8012.
6. Kure, H. I., Islam, S., Mouratidis, H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection // Neural Computing and Applications. 2022. Т. 34, №. 18. Pp. 15241–15271.
7. Tuyishime, E. et al. Enhancing cloud security – proactive threat monitoring and detection using a siem-based approach // Applied Sciences. 2023. Т. 13, №. 22. С. 12359.
8. Краковский Ю. М., Киргизбаев В. П. Системный подход к моделированию работ по устранению инцидентов информационной безопасности применительно к корпоративной информационной системе // Современные технологии. Системный анализ. Моделирование. 2025. № 1(85). С. 116–126.
9. Обеспечение информационной безопасности интегрируемых информационных систем на базе доверия / В. В. Грызунов, А. С. Крюков, А. В. Шестаков, И. А. Зикратов // Труды учебных заведений связи. 2024. Т. 10, № 4. С. 110-125. DOI 10.31854/1813-324X-2024-10-4-110-125.
10. Грызунов В. В. Формирование условия гарантированного достижения цели деятельности информационной системой на базе операторного уравнения // Информатизация и связь. 2022. № 4. С. 67–74. DOI 10.34219/2078-8320-2022-13-4-67-74.
11. Bendicho, C. Cyber security in cloud: Risk assessment models //Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 1 – Cham : Springer International Publishing. 2021. Pp. 471–482. DOI 10.1007/978-3-030-80126-7_32.
12. Battaglioni M. et al. Magic: A method for assessing cyber incidents occurrence //IEEE Access. 2022. Т. 10. Pp. 73458–73473. DOI 10.1109/ACCESS.2022.3190246.
13. Badhwar, R. Simplified Approach to Calculate the Probability of a Cyber Event //The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. – Cham : Springer International Publishing. 2021. Pp. 353–359. DOI 10.1007/978-3-030-79623-5_15.
14. Zängerle, D., Schiereck, D. Modelling and predicting enterprise-level cyber risks in the context of sparse data availability // The Geneva Papers on Risk and Insurance-Issues and Practice. 2023. Т. 48, № 2. С. 434–462. DOI 10.1057/s41288-022-00282-6.

A MULTI-LEVEL FRAMEWORK FOR JUSTIFYING INFORMATION SECURITY INCIDENT MONITORING AND RESPONSE PROCEDURES

Gryzunov V. V.[3], Shestakov A. V.[4]

Keywords: *terminology system, cybersecurity, information security incident management.*

Purpose of the study: *to substantiate approaches for the rational organization of monitoring and response to potential information security incidents.*

Methods of research: *the information system is described by a hierarchical model, developed and tested by the authors, which includes the management level, the personnel level, as well as the hardware and software levels. The model takes as input the sets of possible states of the information system and information security incidents, the admissible values of information security risk probabilities, and the set of admissible control actions. The model outputs a control action that maintains the information security risk probability within a specified range.*

Results: *the multi-level framework provides an end-to-end description of the information security incident management process – from incident detection to the formation of an improvement plan. It allows for quantitative assessment of the effectiveness of response measures at each level of the information system — management, personnel, hardware, and software. A key advantage of the approach is the ability to compensate for the shortcomings of one level by strengthening another, which expands the possibilities for keeping the information security risk probability within a specified range. Based on the obtained assessments, economically justified information security strategies are formed. The central practical conclusion is the principle of "risk redistribution," which replaces the dogmatic requirement to eliminate all vulnerabilities with targeted, measurable, and cost-effective management of the risk probability.*

Scientific novelty: *unlike existing models, the developed model explicitly accounts for the aggregate information security risk probability and the interdependence of all four levels of the information system by forming a corresponding operator.*

References

1. Tokarev V. L. Intellektual'naja podderzhka obnaruzhenija incidentov informacionnoj bezopasnosti / V. L. Tokarev, A. A. Sychugov // Modelirovanie, optimizacija i informacionnye tehnologii. 2023. T. 11, № 1(40). S. 16-17. DOI 10.26102/2310-6018/2023.40.1.006.
2. Kiselev A. A., Praktika sozdanija centra monitoringa informacionnoj bezopasnosti / A. A. Kiselev, I. V. Korotkih, V. V. Shott // Bezopasnost' cifrovyh tehnologij. 2022. T.11, № 1(40). S. 39–51.
3. Olejnikova A. A. Koncepcija upravlenija informacionnoj bezopasnost'ju na osnove cikla nepreryvnogo detektirovanija i reagirovanija na incidenty bezopasnosti informacii / A. A. Olejnikova, V. V. Zolotarev // Izvestija JuFU. Tehnicheskie nauki. – 2023. – № 5(235). S. 66–81. DOI 10.18522/2311-3103-2023-5-66-81.
4. Goncharenko S. N., Lachihina A. B. Monitoring incidentov bezopasnosti geoinformacionnoj sistemy upravlenija i kontrolja dejatel'nosti promyshlennogo predprijatija // Gornyj informacionno-analiticheskij bjulleten' (nauchno-tehnicheskij zhurnal). – 2022. – №. 3. S. 108–116
5. Ma, C. Smart city and cyber-security; technologies used, leading challenges and future recommendations // Energy Reports. 2021. T. 7. S. 7999–8012.
6. Kure, H. I., Islam, S., Mouratidis, H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection // Neural Computing and Applications. 2022. T. 34, №. 18. Rr. 15241–15271.
7. Tuyishime, E. et al. Enhancing cloud security – proactive threat monitoring and detection using a siem-based approach // Applied Sciences. 2023. T. 13, №. 22. S. 12359.
8. Krakovskij Ju. M., Kirgizbaev V. P. Sistemnyj podhod k modelirovaniju rabot po ustraneniju incidentov informacionnoj bezopasnosti primenitel'no k korporativnoj informacionnoj sisteme // Sovremennye tehnologii. Sistemnyj analiz. Modelirovanie. 2025. № 1(85). S. 116-126.
9. Obespechenie informacionnoj bezopasnosti integriruemyh informacionnyh sistem na baze doverija / V. V. Gryzunov, A. S. Krjukov, A. V. Shestakov, I. A. Zikratov // Trudy uchebnyh zavedenij svjazi. 2024. T. 10, № 4. S. 110–125. DOI 10.31854/1813-324X-2024-10-4-110-125.
10. Gryzunov V. V. Formirovanie uslovija garantirovannogo dostizhenija celi dejatel'nosti informacionnoj sistemoj na baze operatornogo uravnenija // Informatizacija i svjaz'. 2022. № 4. S. 67–74. DOI 10.34219/2078-8320-2022-13-4-67-74.
11. Bendicho, C. Cyber security in cloud: Risk assessment models //Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 1 – Cham : Springer International Publishing. 2021. Rr. 471–482. DOI 10.1007/978-3-030-80126-7_32.

3 Vitaly V. Gryzunov, Dr.Sc. of Technical Sciences, Associate Professor, Professor of the Department of Applied Mathematics and Information Technologies of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia. St. Petersburg, Russia. ORCID https://orcid.org/0000-0003-4866-217X. E mail: viv1313r@mail.ru

4 Alexander V. Shestakov, Dr.Sc. of Technical Sciences, Senior Researcher, Leading Researcher of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia. St. Petersburg, Russia. ORCID https://orcid.org/0000-0002-8462-6515. E mail: alexandr.shestakov01@yandex.ru

12. Battaglioni M. et al. Magic: A method for assessing cyber incidents occurrence //IEEE Access. 2022. Т. 10. Rr. 73458-73473. DOI 10.1109/ACCESS.2022.3190246.
13. Badhwar, R. Simplified Approach to Calculate the Probability of a Cyber Event //The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. – Cham : Springer International Publishing. 2021. Rr. 353-359. DOI 10.1007/978-3-030-79623-5_15.
14. Zängerle, D., Schiereck, D. Modelling and predicting enterprise-level cyber risks in the context of sparse data availability // The Geneva Papers on Risk and Insurance-Issues and Practice. 2023. Т. 48, № 2. С. 434–462. DOI 10.1057/s41288-022-00282-6.