Применение функции полезности при выявлении и анализе угроз нарушения информационной безопасности объектов критической информационной инфраструктуры Российской Федерации

Р.Р. Фаткиева, К.З. Билятдинов

***Аннотация*— Предложен подход к обеспечению безопасности объектов критической информационной инфраструктуры, основанный на выявлении и анализе угроз нарушения информационной безопасности с последующим динамическим присваиванием категории значимости ОКИИ путем прогнозирования возможного ущерба за счет оценки изменения целевой функции при возникновении нарушения. Для этого целевая функция минимизации ущерба формализуется в виде иерархического дерева, где корень соответствует общей цели, а дочерние вершины - конкретным подцелям и задачам. Такое представление позволяет учитывать влияние отдельных задач при выполнении целевой функции на процесс категорирования объекта критической инфраструктуры, с возможностью динамического перерасчета категории в случае возникновения угрозы нарушения информационной безопасности. Для прогноза возможных отклонений достижения целевой функции введена функция полезности, позволяющая оценить кумулятивный эффект от возможных нарушений безопасности.**

***Ключевые слова*—целевая функция, угрозы нарушения информационной безопасности, критическая информационная инфраструктура, оценка ущерба, кибербезопасность, коэффициенты критичности, критерии значимости, функция полезности**

I Введение

В условиях увеличения темпов цифровизации и повышения сложности кибератак вопросы обеспечения безопасности объектов критической инфраструктуры (ОКИИ) приобретают важное значение, поскольку нарушение их функционирования влечет масштабные социально-экономические последствия и подрыв устойчивости ключевых отраслей. Процесс управления информационной безопасностью (ИБ) ОКИИ включает этапы: категорирование; построения системы защиты; мониторинга и управления [1, 2]. В этих условиях обеспечение эффективной защиты требует точного определения значимости процессов, протекающих в ОКИИ [3-5]. Ключевым аспектом здесь является то, что критичность процессов не является фиксированной величиной. Изменения внешней и внутренней среды, развитие новых угроз или технологических изменений могут значительно повлиять на категорию значимости анализируемых процессов или компонентов инфраструктуры [6-10]. Кроме того, отсутствие учета взаимосвязей между критическими процессами при их категорировании создает серьезные риски для безопасности ОКИИ [11]. Многие системы в инфраструктуре тесно связаны между собой, и нарушение одного процесса может привести к каскадному эффекту, затрагивающему другие важные процессы, что приводит росту уязвимостей и потерям [12]. Дополнительные сложности при присваивании категории создаются противоречивыми пересечениями в списках критических процессов различных отраслей, что затрудняет выработку единых подходов к их оценке. Традиционные методы управления информационной ИБ, ориентированы на идентификацию изменений в ОКИИ и не затрагивают оценку успешности выполнения целевой функции [13], что приводит к построению модели угроз, не учитывающей динамику изменений, как окружающей среды, так и внутренних состояний ОКИИ. Введение оценки достижения целевой функции в процесс категорирования ОКИИ, позволяет получать динамическую оценку риска нарушения ИБ и своевременно адаптировать стратегии защиты. Это позволит не только минимизировать риски, но и повысить способность ОКИИ адаптироваться к новым угрозам.

II Применение функции полезности при выявлении и анализе угроз нарушения информационной безопасности

К структурно-функциональным особенностям ОКИИ можно отнести наличие сложной вложенной инфраструктуры, декомпозиция которой позволяет получить маршрут достижения стратегических задач, входящих в целевую функцию. В общем виде процесс достижения целевой функции можно представить в виде многоярусной структуры многокритериального представления показателей выполнения задач на каждом

Р.Р. Фаткиева – к.т.н., доцент ПГУПС (email: rikki2@yandex.ru)
К.З. Билятдинов – д.т.н., профессор ГУАП (email: k74b@mail.ru)

из ярусов, либо с использованием различных видов их сверток. В обоих случаях получение набора показателей достижения целевой функции возможно двумя способами: методом декомпозиции, если рассматривать функционирование ОКИИ последовательно «сверху вниз» или методом агрегирования в противном случае. Построение маршрута достижения целевой функции позволяет определить приоритеты для каждой подсистемы ОКИИ, выявить возможные угрозы и «узкие места» и, а также сформировать мероприятия по обеспечению информационной безопасности (ИБ). Тогда в общем виде целевую функцию возможно разделить на два класса:

- функцию, направленную на минимизацию рисков и потерь;

-функцию, направленную на максимизацию конечного результата, частным случаем которой является получение прибыли.

Если рассматривать целевую функцию в контексте функций, направленных на минимизацию рисков и потерь, то перечень показателей критериев значимости инфраструктуры ОКИИ РФ и их значений, возможно объединить в пересекающееся множество, которое объединяется общей функцией минимизации ущерба, наносимого бюджету РФ. В контексте данного рассмотрения целесообразно сформировать подмножество целевых функций с учетом существующего перечня типовых отраслевых ОКИИ как:

$$W_0 = \left\{ W_0^H, W_0^V, W_0^T, W_0^N, W_0^{GA}, W_0^{IA}, W_0^P, W_0^{TR}, W_0^{En} \right\}, \quad (1)$$

где W_0 – целевая функция минимизации ущерба бюджета РФ; W_0^H - функция минимизации причинения ущерба жизни и здоровью людей; W_0^V - функция минимизации ущерба от нарушения функционирования объектов обеспечения жизнедеятельности населения; W_0^T - функция минимизации ущерба от нарушения функционирования объектов транспортной инфраструктуры; W_0^N - функция минимизации ущерба от нарушения функционирования сетей связи; W_0^{GA} - функция минимизации нарушения функционирования государственного органа; W_0^{IA} - функция минимизации ущерба от нарушения условий международного договора; W_0^P - функция минимизации ущерба от снижении уровня дохода; W_0^{TR} - функция минимизации ущерба от нарушения проведения клиентами операций по осуществлению перевода денежных средств; W_0^{En} - функция минимизации ущерба от воздействий на окружающую среду.

Тогда поиск мероприятий по планированию достижения целевой функции отраслевого ОКИИ можно представить, как выбор из двух возможных вариантов:

-минимизации возможных допустимых последствий [14]:

$$W_R = \min \sum_{i=1}^{n} \sum_{k=1}^{m} R_i P_i(t) \quad (2)$$

где n -число рассматриваемых состояний ОКИИ; R_i - возможные предельно допустимые негативные последствия от деструктивных воздействий, выраженные в стоимостном отношении; $P_i(t)$ - вероятность нахождения i –го элемента в k -ом состоянии на момент времени t;

-максимизации возможных допустимых мероприятий по противодействию развития деструктивных воздействий, при минимизации предельно допустимых негативных последствий от них можно выразить в стоимостном отношении как:

$$W_0 = \max \sum_{j=1}^{l} M_j \sum_{k=1}^{m} R_i, \quad (3)$$

где M_j - возможные допустимые мероприятия по противодействию деструктивным воздействиям.

Условия ограничения возможных стоимостных затрат при достижении целевой функции (1) целесообразно представить в виде:

$$\sum_{i=1}^{m} z_{ij}(\lambda_{ij}, t) \le z_{\partial on}, \quad (4)$$

где $z_{ij}(\lambda_{ij}, t)$ -затраты ресурсов на разрешения i-ого деструктивного воздействия при j -ом мероприятии защиты на интервале времени t; $z_{\partial on}$ -допустимые суммарные затраты на разрешение всех деструктивных воздействий на заданном интервале времени.

В свою очередь дальнейшая декомпозиция затрат на ресурсы $z_{ij}(\lambda_{ij}, t)$ позволяет выявить базовые функции управления ресурсами (рис. 1), направленных на:

- минимизацию: затрачиваемых ресурсов (снижение финансовых и операционных затрат при обеспечении ИБ); операционных процессов (повышение эффективности и сокращение избыточных операций); информационных потоков (уменьшение избыточной нагрузки на системы обработки информации); времени выполнения (снижение временных затрат на критические процессы);

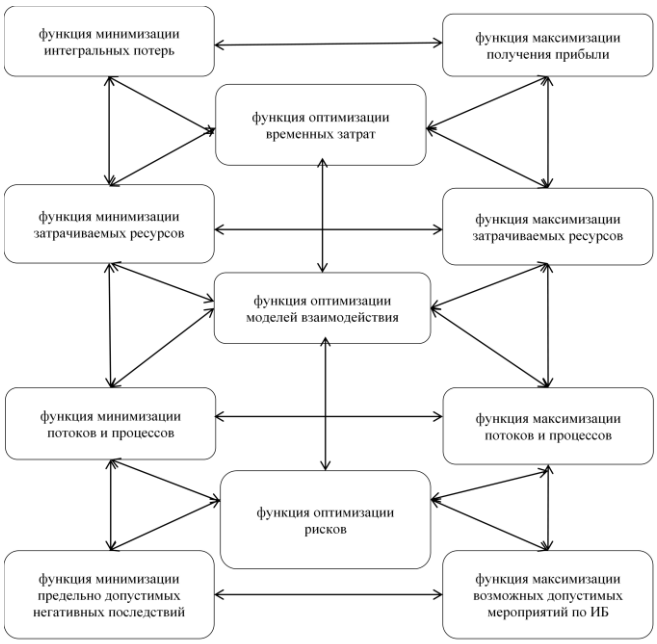

Рис. 1. Декомпозиция функций управления ресурсами

-максимизацию: затрачиваемых ресурсов (усиление безопасности за счет увеличения затрат); операционных процессов (увеличение устойчивости к угрозам за счет дублирования); информационных потоков (возможности обработки данных и быстродействие систем); времени выполнения (обеспечение большей надежности и устойчивости систем); возможных допустимых мероприятий по ИБ (число стратегий защиты).

Однако при более детальном рассмотрении базовых функций управления ресурсами возникает несколько ключевых противоречий, которые влияют на стратегическое управление ОКИИ в процессе достижения им целевой функции (рис. 2). Существующий конфликт между функциями минимизации ресурсов защиты и уровнем защищенности затрудняет обеспечение необходимого уровня безопасности. Так снижение ложных срабатываний может привести к увеличению вероятности пропуска атак, что вызывает конфликт между точностью и полнотой обнаружения угроз. Противоречия между функцией минимизации ущерба и эффективностью средств защиты приводят к ограничениям в функционировании ОКИИ и снижают его эффективность. Точность процесса категорирования ОКИИ требует значительных временных затрат, что снижает оперативность принятия решений и замедляет реакцию на угрозы, создавая конфликт между глубиной анализа и степенью быстроты реагирования.

Рис.2 Виды противоречий в базовых функциях управления ресурсами

Выявленные противоречия требуют нахождения оптимального баланса для эффективного управления рисками и обеспечения безопасности ОКИИ. Поскольку традиционные подходы к защите информации, основанные на локальной оптимизации отдельных параметров, не позволяют полноценно учесть взаимосвязи между различными аспектами безопасности и их влияния на функционирование ОКИИ, то в поиске целевой функции минимизации рисков и потерь (1) целесообразно в качестве маршрута достижения цели ввести дерево целевых функций обеспечения безопасности ОКИИ, которое позволяет систематизировать ключевые направления защиты и выделить базовые управленческие механизмы, которые могут быть использованы для балансировки противоречий между затратами, эффективностью, устойчивостью и уровнем защищенности (рис. 3).

Дерево представляет собой модель, включающую в себя рассмотренные ранее ключевые функции, направленные на минимизацию и/или максимизацию основных ресурсов. Верхний уровень охватывает глобальную функцию минимизации ущерба бюджета РФ согласно (1). На последующих уровнях выделены базовые механизмы управления ресурсами (из перечня, отраженного на рис. 2), такие как: минимизация затрат; время выполнения; количество и виды информационных и операционных потоков; мероприятия по ИБ; устойчивость ОКИИ.

Отличительной особенностью данного подхода является возможность комбинаций базовых функций как внутри отраслей, так и между ними, что позволяет учитывать их взаимное влияние при взаимодействии. Прослеживание пути от корня до листьев на дереве целевых функций дает возможность построить маршрут или маршруты достижения целевой функции. Анализ динамики изменений базовых функциях управления под воздействием угрозы или деструктивного нарушения позволяет проследить степень их влияния на отрасль и на экономику в целом. Оценка данных нарушений обеспечивает формирование вариантов применения средств защиты информации, а также выявляет критические противоречия между требованиями безопасности и экономической эффективности. Это в свою очередь дает возможность разрабатывать сбалансированные стратегии защиты ОКИИ с учетом

специфики ИБ и особенностей его функционирования. При этом следует учитывать, что рассмотренные на рисунках и 1 и 3 функции так или иначе связаны с необходимостью передачи информации, то есть обеспечения безопасности информационного потока. Ограничимся в дальнейшем рассмотрении ими. Для формирования целевой функции W_0^N направленной на минимизацию риска сбоев в сетевой инфраструктуре ключевыми параметрами управления согласно дереву достижения цели (рис. 3) выступают: $W^N_{МПДНП}$ - минимизация предельно допустимых негативных последствий; $W^N_{МРПТ}$ -минимизация рисков перехвата трафика; $W^N_{МАИТ}$ – минимизация вероятности сетевых атак; $W^N_{МИП}$ – максимизация количества информационных потоков с полезной нагрузкой; $W^N_{МВДПИБ}$ – максимизация возможных допустимых мероприятий по ИБ; $W^N_{МОС}$ – максимизация отказоустойчивости сетевой инфраструктуры.

Прохождение дерева с анализом представленных функций позволяет сформировать пример частной целевой функции W_0^N , с учетом базовых функций как:

$$W_0^N = f_1(W^N_{МИП},\ W^N_{МВДПИБ},\ W^N_{МОС}) + f_2(W^N_{МПДНП},\ W^N_{МРПТ},W^N_{МАИТ}) \quad (5)$$

при ограничениях:

$$W^N_Z < W^N_{МПДНП},$$
$$W^N_N > W^N_{МИП},$$
при условии $W^N_{МВДПИБ} < W^N_Z$
$$W^{MAX}_{МАИТ} > W^N_{МАИТ},$$
$$W^N_{МОС} > W^{MIN}_{МОС}, \text{ при условии } W^N_{МВДПИБ} < W^N_Z,$$

где f_1, f_2 функция затрат; $W^N_{МПДНП}$ -затраты на устранение предельно допустимых негативных последствий; $W^N_{МРПТ}$ -затраты на устранение риска перехвата трафика; $W^N_{МАИТ}$ – затраты на уменьшения вероятности сетевых атак; $W^N_{МИП}$ – затраты на увеличение количества информационных потоков с полезной нагрузкой; $W^N_{МВДПИБ}$ – затраты на

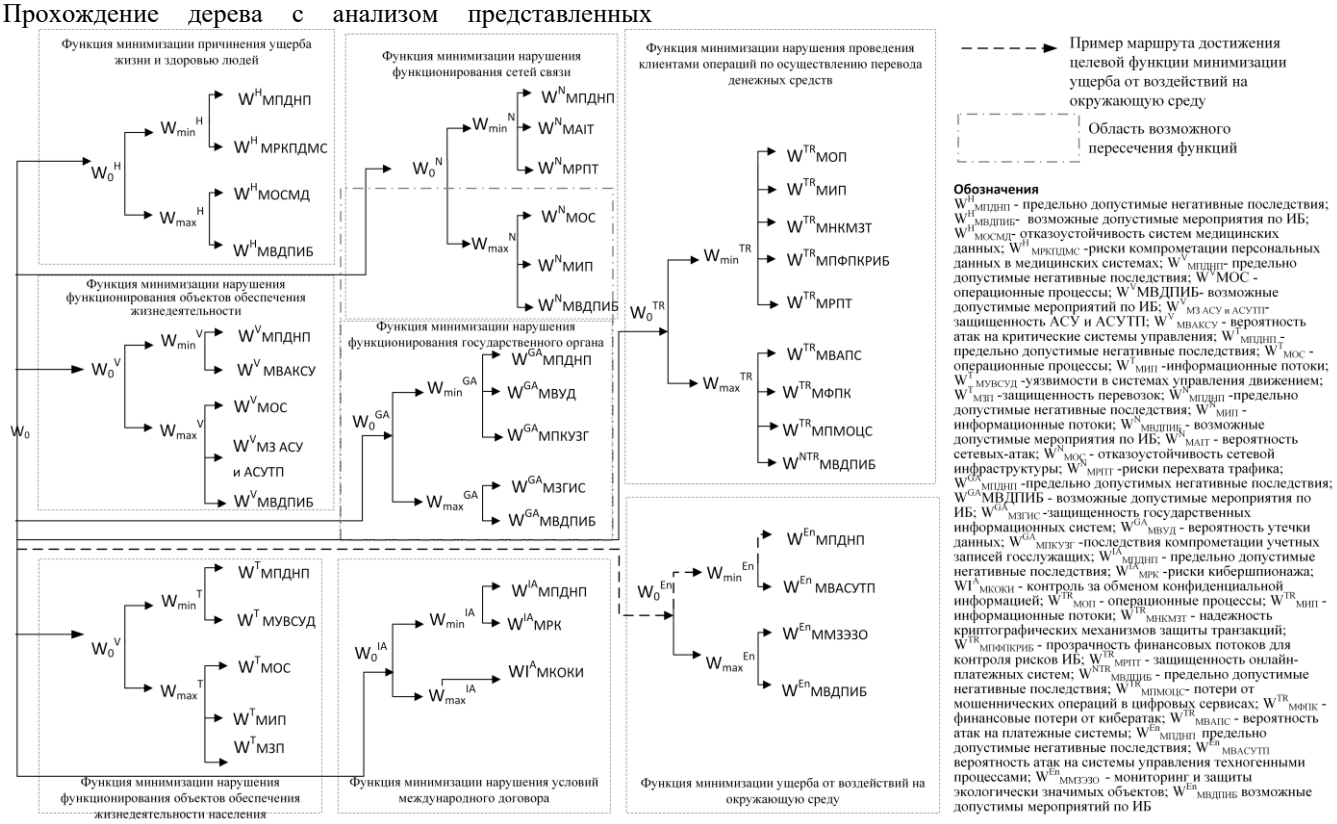

Рис.3 Дерево достижения целевых функций

мероприятия по ИБ; $W^N_{МОС}$ – затраты на обеспечение отказоустойчивости сетевой инфраструктуры; W^N_Z – затраты на средства обеспечения ИБ; W^N_N – пропускная способность сетевой инфраструктуры; $W^{MAX}_{МАИТ}$ - максимально допустимый уровень вероятности атак; $W^{MIN}_{МОС}$ - минимально допустимый уровень отказоустойчивости.

Исходя из (5) и нормативно-правовой базы возникает необходимость достижения баланса при формировании целевой функции с учетом обеспечения целостности, доступности и конфиденциальности информации в процессе ее передачи в сетевой инфраструктуре с одной стороны и необходимостью выявления критических процессов, в которых она участвуют за счет обеспечения категорирования, мониторинга и реконфигурации процессов обработки с другой стороны (рис. 4).

Основным процессом при категорировании ОКИИ является определение значимости критических процессов, то есть уровня влияния угроз, происходящих в нем на целевую функцию.

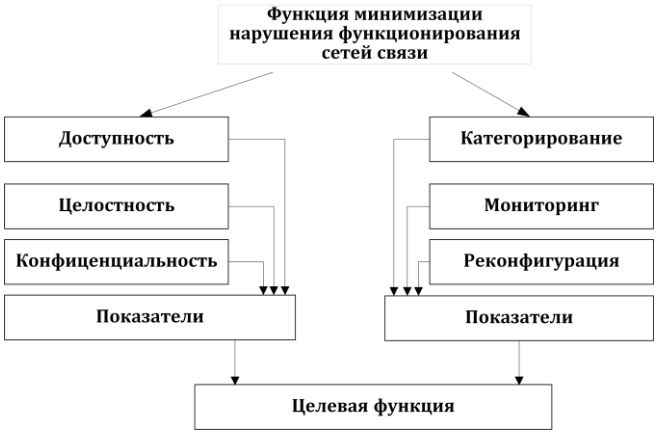

Рис.4 Показатели функционирования сетей связи

Значимость процессов, протекающих в ОКИИ определен как совокупность параметров, отражающих его влияние через определение ущерба, наносимого угрозами ИБ:

$$K = \prod_{i=1}^{N} K_i (У_i \cdot P_i), \qquad (6)$$

где K-категория значимости оцениваемого процесса; K_i - коэффициент критичности i-го рассматриваемого процесса; $У_i$ - возможный ущерб при нарушении безопасности оцениваемого i-го процесса (в рассматриваемом случае с учетом того, что ущерб зависит от затрат на обеспечение безопасности $У_i(W_0^N)$; P_i - вероятность нарушения процесса.

Отметим, что в частном случае функция (6) является функцией полезности Стоун–Гири:

$$K = \prod_{i=1}^{N} (k_i - \gamma_i)^{a_i}, \qquad (7)$$

k_i - фактическое значение i-го показателя критичности процесса; γ_i - порог для показателя критичности процесса; a_i - вес процесса, учитывающего его важность. Нетрудно заметить, что при $a_i = 1$ (7) превращается в функцию, используемую при традиционном подходе (6).

Очевидно, что чем выше значимость оцениваемого процесса, тем серьезнее последствия его отказа, в связи с чем возникает необходимость в приоритезации мер защиты, в зависимости от возможного ущерба. Однако в этих условиях процесс получения категории значимости ОКИИ осложняется рядом противоречий, обусловленных необходимостью достижения равновесия между точностью анализа, оперативностью принятия решений и доступными для оценивания ресурсами (рис 5). Учет значительного количества угроз позволяет повысить достоверность категорирования, но при этом увеличивает время их обработки, что затрудняет своевременность принятие решений. Особенно это актуально в условиях динамически меняющего ландшафта угроз.

Рис. 5. Взаимосвязь характеристик процесса категорирования

С другой стороны, высокая степень защищенности ОКИИ может не отражать его критическую значимость, тогда как анализ менее защищенных объектов может привести к ложным срабатываниям и перерасходу ресурсов. При этом детальный анализ угроз требует значительных вычислительных и кадровых затрат, а их

нехватка приводит к упрощению модели угроз, что также снижает точность категорирования. Кроме того, высокая степень детализации позволяет точнее определить уровень значимости объектов, однако усложняет оперативную адаптацию системы защиты и принятие решений в изменяющихся условиях угроз. Наконец, существует конфликт между централизованным управлением процесса категорирования, обеспечивающим единые критерии оценки, и автономным управлением, позволяющем оперативно реагировать на локальные риски. Эти противоречия требуют разработки подходов, позволяющих находить баланс между полнотой анализа, эффективностью защиты и оперативностью реагирования.

С учетом этого возникает необходимость расширения подхода категорирования, представленного в (6), (7) введением дополнительных характеристик (табл. 1), позволяющих более точно осуществить категорирование критических процессов за счет снижения риска пропущенных угроз и уязвимостей за счет анализа противоречий в анализируемом объекте.

С практической точки зрения введение дополнительных характеристик позволяет дополнить дерево целевых функций обеспечения безопасности ОКИИ (рис. 3, табл 1), что в свою очередь дает более полную картину для оценки ущерба:

$$W_0^N = f_1(W^N_{МИП}, W^N_{МВДПИБ}((K^{min}_{ОП}, K^{max}_{УЗО})), W^N_{МОС}) + f_2(W^N_{МПДНП}, W^N_{МРПТ}, W^N_{МАИТ}(K^{max}_{ППУ}(K^{max}_{Р}))) \quad (8)$$

Однако подход, представленный в (6) не позволяет с одной стороны оперативно получать категорию значимости процесса, при изменении ландшафта угроз, что влечет за собой задержку в формировании мероприятий по достижению заданного уровня безопасности и учета введенных на этапе получения целевой функции ограничений и противоречий с другой стороны. Более того, противоречия, определенные на этапе получения целевой функции, могут становиться менее актуальными в условиях динамичного изменения угроз, что требует дополнительной анализа процесса категорирования и адаптации модели управления рисками и ее интеграции с системами мониторинга угроз в реальном времени.

В этих условиях использование (6) ограничено пороговыми значениями, поскольку в случае отдельно взятого показателя, для которого выполняется условие $k_i = \gamma_i$ мультипликативная свертка перестает отражать текущее положение ИБ и не учитывает дополнительные характеристики из таблицы 1.

Таблица 1. Дополнительные задачи процесса категорирования

Характеристика	**Задача минимизации показателей**	**Задачи максимизации показателей**
Полнота учета угроз	$K^{min}_{ППУ} = \min \sum_{j=1}^{N} Y_j(t)$, где Y_j -угроза нарушения ИБ	$K^{max}_{ППУ} = \max \sum_{j=1}^{N} Y_j(t)$, где Y_j -угроза нарушения ИБ
Оперативность выявления	$K^{min}_{ОП} = \min \sum_{i=1}^{M} (T_i \cdot x_i), T_i \le T_{max} \cdot T_i$ - время, необходимое для выявления нарушения *i*-ого объекта, которое не должно превышать допустимое T_{max} время; x_i -бинарная переменная, показывающая, выбран ли объект для выявления (0 – если не выбран, 1- в противном случае), в частном случае $T_i = K^{min}_{Ta}$.	$K^{max}_{ОП} = \max(\sum_{j=1}^{N} Y_j(t), \sum_{i=1}^{M} (T_i \cdot x_i))$ - показатель задан как увеличение количества анализируемых угроз при заданном времени обнаружения
Уровень защищенности объектов	$K^{min}_{УЗО} = \min \sum_{k=1}^{L} Z_k(t)$, где - затраты Z_k для *k*-го средства защиты	$K^{max}_{УЗО} = \max \sum_{k=1}^{L} Z_k(t)$, где - затраты Z_k для *k*-го средства защиты
Вероятность выявления нарушений	$P = \min \sum_{j=1}^{Y} O_j(P_j)$ где $O_j(P_j)$ - ложные срабатываний	$K^{min}_{ЛС} = \min \sum_{j=1}^{Y} (\Delta P_j(Y_j) \cdot x_j)$, при условии $\lim_{n \to \infty} \Delta P = 0$, где $\Delta P_j(Y_j)$ -абсолютная погрешность вероятности *j*-го ложного срабатывания; *n*-количество ложных срабатываний
Ограничения на ресурсы	$K^{min}_{ЗР} = \min(\sum_{l=1}^{L} R_l) / R,$ где R_l - задействованные ресурсы; R - общее количество ресурсов	$K^{max}_{ЗР} = \max(\sum_{l=1}^{L} R_l) / R,$ где R_l - задействованные ресурсы; R - общее количество ресурсов
Степень детализации	$K^{min}_{Д} = \min(\sum_{v=1}^{Q} D_v) / D,$ где D_v -анализируемый *v*-ый процесс ОКИИ; D - общее количество рассматриваемых процессов	$K^{max}_{Д} = \min(\sum_{v=1}^{Q} D_v) / D,$ где D_v -анализируемый *v*-ый процесс ОКИИ; D - общее количество рассматриваемых процессов

Показатель гибкости и скорости реагирования	$K_{ГСР}^{\min} = \min(((\sum_{j=1}^{N} \text{Sec}_j(t) / \sum_{j=1}^{N} Y_j(t)), K_{ЗСЗИ})$, где Sec_j - СЗИ от *j*-ой угрозы; $K_{ЗСЗИ}$ -затраты внедрения СЗИ	$K_{ГСР}^{\max} = \max(\sum_{j=1}^{N} Y_j(t) / \sum_{j=1}^{N} \text{Sec}_j(t))$ при условии $\min K_{ЗСЗИ}$, где Sec_j - СЗИ от *j*-ой угрозы; $K_{ЗСЗИ}$ - затраты внедрения СЗИ
Автономность средств управления (централизованность управления)	$K_{КАСУ}^{\min} = \min N_{авт}(\text{Sec}) / \max N_{цент}(\text{Sec})$ где $N_{авт}(\text{Sec})$ - количество автономных СЗИ; $N_{цент}(\text{Sec})$ - количество управляемых СЗИ	$K_{КАСУ}^{\max} = \max N_{цент}(\text{Sec}) / \min N_{авт}(\text{Sec})$, где $N_{авт}(\text{Sec})$ - количество автономных СЗИ; $N_{цент}(\text{Sec})$ - количество управляемых СЗИ

В связи с этим осуществим переход от функции Стоун-Гири к квазилинейной функции полезности. Для этого применим натуральный логарифм к обеим частям:

$$\ln K = \ln(\prod_{i=1}^{N}(k_i - \gamma_i)).$$

Переопределим разность $k_i - \gamma_i$ как $z_i = k_i - \gamma_i$, $z_i > 0$. Используя свойство логарифма произведения и степени, получим:

$$\ln K = \sum_{i=1}^{N} \ln z_i .$$

Зафиксируем все z_i, для $i < N$ на уровне близком к Y_i и разложим z_i в ряд Тейлора:

$$\ln z_i \approx \ln \varepsilon_i + \frac{z_i - \varepsilon_i}{\varepsilon_i}, \varepsilon_i \to 0.$$

Для z_N, линейный член $\ln z_N = z_N - 1$, при $z_N \to 0$ получим:

$$\ln K \approx \sum_{i=1}^{N-1} (\ln \varepsilon_i + \frac{z_i - \varepsilon_i}{\varepsilon_i} - 1) + (z_N - 1)$$

Для возврата к K осуществим экспоненцирование, пренебрегая константой $(\ln \varepsilon_i - 1)$:

$$K \approx \exp \sum_{i=1}^{N-1} \frac{z_i}{\varepsilon_i} + z_N$$

Положим, что $\varepsilon_i = 1$ для всех i, и используя приближение $e^y \approx 1 + y$ получим:

$$K \approx 1 + \sum_{i=1}^{N-1} z_i + z_N$$

Поскольку константа 1 не влияет на оценку функционирования исследуемого объекта, поэтому ею можно пренебречь:

$$K \approx \sum_{i=1}^{N-1} z_i + z_N$$

Подставив $z_i = k_i - \gamma_i$ и $z_N = k_N$ получим:

$$K \approx \sum_{i=1}^{N-1} (k_i - \gamma_i) + k_N \quad (9)$$

Переход от функции Стоун-Гири к квазилинейной функции полезности позволяет учитывать процессы, протекающие в ОКИИ и динамически отслеживать нарушения как для одного оцениваемого процесса, так и для всей системы в целом.

III Практическое применение

В качестве иллюстрации осуществим моделирование поведение функции полезности (9) и определение критичности (6) для оценки одного процесса обработки информации в инфраструктуре предприятия за промежуток времени t_1-t_{10} (табл. 2, рис. 6).

Кривая функция полезности фактически повторяет поведение кривой отклонений от пороговых значений за исключением следующих ситуаций:

-если расхождение между кривой отклонений и кривой функции полезности $\Delta K > 0$ – то имеет место превышение верхнего уровня порогового значения;

- если расхождение между кривой отклонений и кривой функции полезности $\Delta K < 0$, то в процессе функционирования имеет место снижение процесса передачи данных ниже уровня минимального порогового значения;

Таблица 2. Пример оценки функции полезности для одного процесса во времени

Время	**Присваиваемая категория**	**Максимально допустимое время, в течение которого информационная система может быть недоступна пользователю (часов)**	**Пороговое значение времени обработки операции**	**Фактическое значение времени обработки операции**	**Значение отклонения**	**Значение функции полезности**
t_1	1	2	2	3	1	1
t_2	2	2	4	2	-2	-1
t_3	2	3	5	7	2	1
t_4	Процесс не учитывается как критический	2	3	3	0	1

t_5	Процесс не учитывается как критический	2	4	4	0	1
t_6	2	2	5	7	2	3
t_7	Процесс не учитывается как критический	3	1	1	0	3
t_8	1	2	3	4	1	4
t_9	Процесс не учитывается как критический	4	2	2	0	4
t_{10}	1	4	3	2	-1	3

- если расхождение между кривой отклонений и кривой критичности одновременно $\Delta K = 0$, то это свидетельствует о начале нового нарушения. Однако подход, основанный на оценке только одного процесса, не позволяет осуществить оценку нарушений функционирования всего ОКИИ при возможной корреляции между процессами. Не меняя значений отклонений для этого процесса, осуществим комплексную оценку обработки информационного потока внутри ОКИИ, имеющим в своем составе 5 узлов, с учетом задержек обработки, выраженных в часах (табл. 3).

Накопленная сумма нарушений, отраженная в функции полезности (красная кривая на рис. 7) позволяет не только оперативно выстроит систему категорирования, но оценить масштаб нарушения.

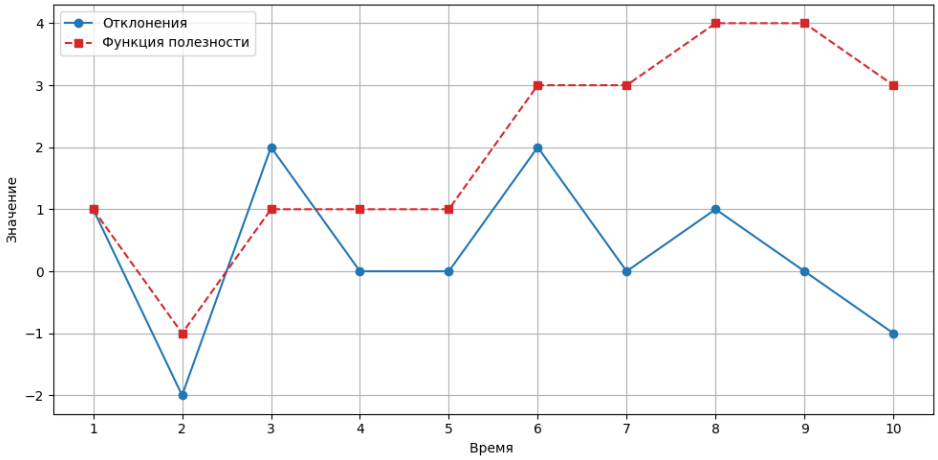

Рисунок 6. Моделирование поведения функции полезности для одного процесса передачи информации

Таблица 3. Значения отклонений для пяти процессов исследуемого объекта при нарушении функционирования

Значения отклонения в обработки информации, час					**Функция полезности**
1	**2**	**3**	**4**	**5**	
1	0	0	2	1	4
-2	1	0	2	2	11
2	2	0	0	0	12
0	-1	4	-1	4	22
0	2	-2	0	-1	23
2	3	3	-1	4	36
0	-1	1	1	1	39
1	0	0	3	0	42
0	-1	0	-1	0	40
-1	0	1	0	0	41

Как видно из рисунка 7 отклонения всех процессов находятся в диапазоне от - 2 часов уменьшение времени обработки до +4 часов увеличения временного интервала обработки информации, что не учитывает кумулятивный эффект, сформированный от суммарного временного интервала отклонений на маршруте достижения целевой функции, что приводит к неправильной идентификации возможного ущерба. Рассмотрение функции полезности в рамках (9) для всех процессов, позволяет вводить накопленный эффект от всех выявленный нарушений на промежутке временного интервала от времени t_1 до t_{10}, что дает возможность более точно спрогнозировать ущерб за рассматриваемый промежуток времени и на основании этого оптимизировать маршрут достижения целевой функции.

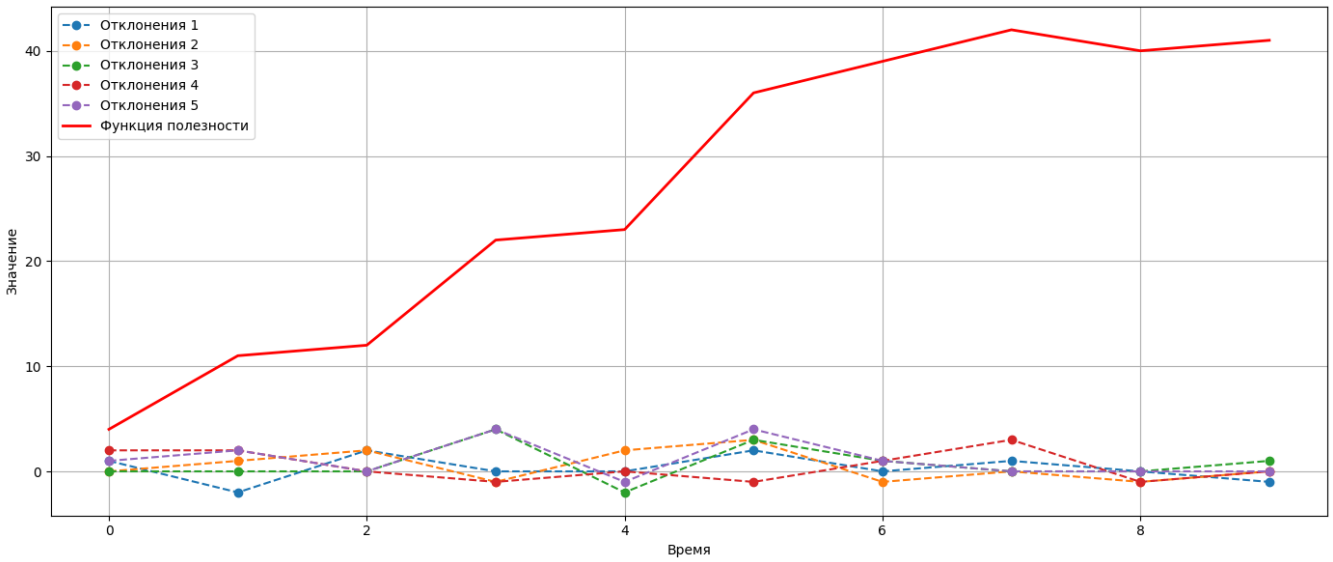

Рисунок 7. Пример поведения функции полезности для 5 процессов обработки информации

К дополнительных характеристикам, учитываемым в (9) в качестве переменной k_N целесообразно отнести влияние уровня защищенности; сбоев и их последствия; время восстановления; скорость реакции на инциденты; и другие характеристики, влияющие на обработку информации.

IV Заключение

Полученные в исследовании результаты показали, что рассмотрение вопросов обеспечения безопасности ОКИИ с учетом введения функции полезности, основанной на оценке достижения целевой функции, при воздействии угроз позволяет осуществить динамический прогноз ущерба как для объекта критической инфраструктуры, так и отрасли в целом. Применение прогноза возможного ущерба применительно к процессам категорирования позволяет перейти к динамическому присваиванию категории значимости ОКИИ. К дальнейшим направлениям исследования целесообразно отнести введение функции полезности при разработке методов мониторинга и управления информационной безопасностью ОКИИ.

Библиография

[1] Roshanaei, M. (2021) Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. Journal of Computer and Communications, 9, 80-102. doi: 10.4236/jcc.2021.98006.

[2] Аудит и мониторинг состояния объектов информатизации в процессе проектирования комплексных систем защиты информации значимых объектов критической информационной инфраструктуры / М. Ю. Рытов, Н. О. Мусиенко, Ю. А. Губсков, Ю. В. Минин // Приборы и системы. Управление, контроль, диагностика. – 2022. – № 10. – С. 10-18. – DOI 10.25791/pribor.10.2022.1364.

[3] Репьева В. Д. Особенности и проблемы категорирования объектов критической информационной инфраструктуры / В. Д. Репьева, А. Х. Ханмагомедов // Вестник науки. – 2023. – Т. 5, № 1(58). – С. 193-196.

[4] Наталичев Р. В., Горбатов В. С., Гавдан Г. П., Дураковский А. П. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры // Безопасность информационных технологий. – 2021. – Т. 28, № 3. – С. 6-27. – DOI 10.26583/bit.2021.3.01.

[5] Зайка В. М. Обеспечение безопасности объекта критической информационной инфраструктуры / В. М. Зайка // Вестник науки. – 2024. – Т. 4, № 10(79). – С. 750-758.

[6] Цыпкина А. В. Применение вероятностного метода оценки опасности объектов КИИ при возникновении чрезвычайных ситуаций / А. В. Цыпкина, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2023. – Т. 6, № 1. – С. 284-290. – DOI 10.33764/2618-981X-2023-6-4-290.

[7] Петров М. Ю., Фаткиева Р. Р. Модель синтеза распределенных атакующих элементов в компьютерной сети // Труды учебных заведений связи. – 2020. – Т. 6, № 2. – С. 113-120. – DOI 10.31854/1813-324X-2020-6-2-113-120.

[8] Мельников А. В., Чирков В. Е. Классификация каналов утечки конфиденциальной информации для моделирования значимости объектов критической информационной инфраструктуры // Охрана, безопасность, связь. – 2019. – № 4-2. – С. 139-144.

[9] Фоменко К. Э., Кущев А. В. Модель обеспечения информационной безопасности элементов критической информационной инфраструктуры на основе онтологического подхода в условиях деструктивных воздействий // Электронный сетевой политематический журнал «Научные труды КубГТУ». – 2022. – № 3. – С. 25-33.

[10] Кубарев А. В., Лапсарь А. П., Федорова Я. В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. – 2020. – № 1(35). – С. 8-17. – DOI 10.21681/2311-3456-2020-01-08-17.

[11] Категорирование взаимосвязанных объектов критической информационной инфраструктуры / Д. М. Малиничев, Х. Х. Кучмезов, В. В. Мочалов [и др.] // Прикладная информатика. – 2022. – Т. 17, № 3(99). – С. 105-116. – DOI 10.37791/2687-0649-2022-17-3-105-116.

[12] Байбеков А. Т. Экономическое моделирование последствий масштабных кибератак на критическую инфраструктуру: оценка системного риска для национальной экономики / А. Т. Байбеков, Н. Е. Лесникова // Журнал монетарной экономики и менеджмента. – 2025. – № 11. – С. 337-340. – DOI 10.26118/2782-4586.2025.16.58.043.

[13] Fatkieva R.R. Systems of Information Security Indicators for Industrial Enterprises. *Autom. Doc. Math. Linguist.* **53**, 216–224 (2019). https://doi.org/10.3103/S000510551904006X.

[14] Евневич Е. Л., Фаткиева Р. Р. Моделирование информационных процессов в условиях конфликтов // Вопросы кибербезопасности. – 2020. – № 2(36). – С. 42-49. – DOI 10.21681/2311-3456-2020-2-42-49.

Application of the utility function in the identification and analysis of threats to the information security of objects of the critical information infrastructure of the Russian Federation

R.R. Fatkieva, K.Z. Bilyatdinov

***Abstract*— An approach to ensuring the security of critical information infrastructure facilities is proposed, based on the identification and analysis of threats to information security violations, followed by the dynamic assignment of a category of significance to the OKII by predicting possible damage by assessing changes in the target function when a violation occurs. To do this, the damage minimization objective function is formalized as a hierarchical tree, where the root corresponds to a common goal, and the child vertices correspond to specific sub-goals and tasks. This representation allows you to take into account the impact of individual tasks when performing the objective function on the process of categorizing an object of critical infrastructure, with the possibility of dynamically recalculating the category in the event of a threat to information security. To predict possible deviations in achieving the target function, a utility function has been introduced to assess the cumulative effect of possible security breaches.**

***Keywords*—objective function, information security threats, critical information infrastructure, damage assessment, cybersecurity, criticality coefficients, significance criteria, utility function.**

REFERENCES

[1] Roshanaei, M. (2021) Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. Journal of Computer and Communications, 9, 80-102. doi: 10.4236/jcc.2021.98006.

[2] Rytov M. Y., Musienko N. O., Gubskov Yu. A., Minin Yu. V. Audit and monitoring of the state of informatization facilities in the process of designing integrated information security systems for significant critical information infrastructure facilities. *Devices and Systems. Management, monitoring, diagnostics.* 2022, no. 10, pp. 10-18. (In Russ.) DOI 10.25791/pribor.10.2022.1364.

[3] Repyeva V. D., Khanmagomedov A. H. Features and problems of categorizing objects of critical information infrastructure. *Bulletin of Science*, 2023, Vol. 5, no. 1(58), pp. 193-196. (In Russ.).

[4] Natalichev R. V., Gorbatov V. S., Gavdan G. P., Durakovsky A. P. Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities. *Information technology security*, 2021, Vol. 28, no. 3, pp. 6-27. (In Russ.). DOI 10.26583/bit.2021.3.01.

[5] Zaika V. M. Ensuring the security of a critical information infrastructure facility. *Bulletin of Science*, 2024, Vol. 4, no. 10(79). – pp. 750-758. (In Russ.).

[6] Tsypkina A.V., Shaburova V. N. Application of a probabilistic method for assessing the danger of CII objects in emergency situations. *Interexpo Geo-Siberia*, 2023, Vol. no. 6 (1), No. pp 284-290. (In Russ.). DOI 10.33764/2618-981X-2023-6-4-290 .

[7] Petrov M, Fatkieva R. A Model of Synthesis of Distributed Attacking Elements in a Computer Network. *Proceedings of Telecommunication Universities*. 2020;6(2):113-120. (In Russ.) https://doi.org/10.31854/1813-324X-2020-6-2-113-120

[8] Melnikov A.V., Chirkov V. E. Classification of confidential information leakage channels for modeling the significance of critical information infrastructure facilities. *Security, safety, communications*, 2019, no. 4-2, pp. 139-144. (In Russ.)

[9] Fomenko K. E., Kushchev A.V. A model for ensuring information security of critical information infrastructure elements based on an ontological approach in conditions of destructive influences. *Scientific works of KubSTU*, 2022, no. 3, pp. 25-33. (In Russ.).

[10] Kubarev A.V., Lapsar A. P., Fedorova Ya. V. Improving the safety of operation of significant critical infrastructure facilities using parametric models of evolution. *Cybersecurity issues*.,2020; № 1(35), pp. 8-17. (In Russ.). DOI 10.21681/2311-3456-2020-01-08-17.

[11] Malinichev D. M., Kuchmezov H. H., Mochalov V. V. [et al.]. Categorization of interconnected objects of critical information infrastructure. *Applied Informatics*, 2022, Vol. 17, no. 3(99), pp. 105-116. (In Russ.). DOI 10.37791/2687-0649-2022-17-3-105-116.

[12] Baibekov A. T., Lesnikova N. E. Economic modeling of the consequences of large-scale cyber-attacks on critical infrastructure: assessment of systemic risk for the national economy. *Journal of Monetary Economics and Management*, 2025.no. 11, pp. 337-340. (In Russ.). DOI 10.26118/2782-4586.2025.16.58.043.

[13] Fatkieva, R.R. Systems of Information Security Indicators for Industrial Enterprises. *Autom. Doc. Math. Linguist.* 53, 216–224 (2019). https://doi.org/10.3103/S000510551904006X.

[14] Evnevich E. L., Fatkieva R. R. Modeling information processes in conflict conditions. Cybersecurity issues, 2020, № 2(36), pp. 42-49. (In Russ.). DOI 10.21681/2311-3456-2020-2-42-49.

Статья получена 3 февраля 2026.