УДК 004
https://doi.org/10.31854/2307-1303-2025-13-4-15-30
EDN: TTTFWO

Методический подход к определению надежности исполнителя мероприятий плана реагирования на компьютерные инциденты на значимых объектах критической информационной инфраструктуры

Комаров В. В.

Научно-исследовательский институт организации здравоохранения и медицинского менеджмента Департамента здравоохранения города Москвы,
Москва, 115088, Российская Федерация

Целью *исследования является определение надежности работника субъекта критической информационной инфраструктуры, задействованного в реализации мероприятий по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак на значимые объекты указанной инфраструктуры, а также оценка целесообразности использования данного параметра, характеризующего исполнителя, в системах поддержки принятия решений. В рамках решения* ***задачи*** *назначения ответственных исполнителей упомянутых мероприятий предложен* ***методический подход*** *по определению надежности исполнителя плана реагирования на компьютерные инциденты. Проведены практические экспериментальные исследования по оценке эффективности действий работников субъектов критической информационной инфраструктуры, имеющих разную квалификацию и навыки. В* ***результате*** *исследования предложен подход к расчету основных показателей квалификации и навыков исполнителя, а также использованию полученных показателей при решении задачи распределения исполнителей (задача о назначениях), что позволит сократить время реагирования на компьютерный инцидент и ликвидацию последствий компьютерной атаки. Полученные результаты позволяют обоснованно сформировать требования к квалификации и навыкам персонала сил безопасности значимых объектов критической информационной инфраструктуры и обеспечить взаимозаменяемость исполнителей.* ***Практическая значимость*** *исследования заключается в решении задачи оптимального распределения (назначения) исполнителя с учетом его квалификации и навыков при реагировании на компьютерные инциденты и ликвидации последствий компьютерных атак.*

Ключевые слова: *критическая информационная инфраструктура, объект критической информационной инфраструктуры, компьютерный инцидент, модель, компьютерная атака*

Введение

Определяя основные обязанности субъектов критической информационной инфраструктуры (КИИ), федеральное законодательство предписывает вы-

Библиографическая ссылка на статью:
Комаров В. В. Методический подход к определению надежности исполнителя мероприятий плана реагирования на компьютерные инциденты на значимых объектах критической информационной инфраструктуры // Информационные технологии и телекоммуникации. 2025. Т. 13. № 4. С. 15–30. DOI: 10.31854/2307-1303-2025-13-4-15-30. EDN: TTTFWO

Reference for citation:
Komarov V. A Methodological Approach to Determining the Reliability of the Executor of the Computer Incident Response Plan at Significant Facilities of Critical Information Infrastructure // Telecom IT. 2025. Vol. 13. Iss. 4. PP. 15–30. (in Russian). DOI: 10.31854/2307-1303-2025-13-4-15-30. EDN: TTTFWO

полнять требования не только по обеспечению безопасности ее значимых объектов, но и по реагированию на компьютерные инциденты[1]. В 2025 г. вышеуказанные требования были распространены на иные органы (организации) Российской Федерации, не относящиеся к субъектам КИИ[2].

Основная цель деятельности по реагированию на компьютерные инциденты – это снижение уровня их потенциальных негативных воздействий на критические процессы, нарушение и (или) прекращение которых может привести к отрицательным социальным, политическим, экономическим, экологическим последствиям, а также последствиям в сфере обеспечения обороны страны, безопасности государства и правопорядка, финансовым потерям или долгосрочным убыткам из-за испорченной репутации и потери доверия к организации[3].

Для подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом КИИ разрабатывается план реагирования и принятия мер по ликвидации последствий (далее – План)[4]. Аналогичный подход присутствует в международных стандартах информационной безопасности[5].

Эффективность деятельности по реагированию на компьютерные инциденты зависит от квалификации привлекаемых специалистов (далее – исполнителей). С учетом роли исполнителя при реализации Плана и особенностей технологических процессов субъекта КИИ определяется необходимый объем его знаний и навыков. В субъектах КИИ рекомендуется вести реестр исполнителей, содержащий следующую информацию:

– перечень работников, которые могут быть привлечены к реагированию на компьютерные инциденты;

– перечень знаний, навыков и умений, которыми обладают эти работники[6]. При этом необходимо учитывать, что исполнителям может потребоваться различный уровень подготовки в зависимости от выполняемых ими задач в соответствии

---

[1] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[2] Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации».

[3] ГОСТ Р 59710-2022. Национальный стандарт Российской Федерации. Защита информации. Управление компьютерными инцидентами. Общие положения. М.: Российский институт стандартизации, 2022. 11 с.

[4] Приказ ФСБ России от 25 декабря 2025 г. № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[5] ISO/IEC 27031:2025 Cybersecurity – Information and communication technology readiness for business continuity. URL: https://cdn.standards.iteh.ai/samples/80975/8e844992be7e4ec88c4c364d22e73a4f/ISO-IEC-27031-2025.pdf

[6] ГОСТ Р 59710-2022. Национальный стандарт Российской Федерации. Защита информации. Управление компьютерными инцидентами. Общие положения. М.: Российский институт стандартизации, 2022. 11 с.

с Планом, что создает дополнительные трудности при перераспределении обязанностей и полномочий в условиях компьютерного инцидента и обеспечения взаимозаменяемости в случае отсутствия (недоступности) основных исполнителей[7].

Руководитель субъекта КИИ должен быть проинформирован о расхождении критических возможностей плановой готовности информационно-коммуникационных технологий организации к обеспечению непрерывности бизнес-процессов, включая расхождения в требуемом уровне знаний и навыков исполнителей[8]. Под надежностью исполнителя мероприятий Плана в рамках данной работы подразумевается способность человека выполнить задачу в заданных условиях в пределах установленного периода времени с учетом заданных ограничений[9] [1].

Так как реальная работа подразделений безопасности субъектов КИИ осуществляется в условиях неопределенности, эффективное управление при реагировании на компьютерные инциденты необходимо основывать на информационных технологиях поддержки принятия решений [2]. Практическая реализация подобных технологий осуществляется в системах поддержки принятия решений (СППР) [3], целевое назначение которых состоит в формировании необходимой альтернативы среди множества вариантов при принятии ответственных решений [4].

Математическое обеспечение СППР позволяет принимать специалисту по информационной безопасности обоснованные и оптимальные решения для обеспечения безопасности значимых объектов КИИ, а различные вероятностные и статистические методы – анализировать неопределенность и управлять оценкой вероятности различных сценариев потенциальных последствий компьютерных атак [5]. Основное назначение процессов управления – это своевременная выработка и доведение необходимого воздействия на управляемый объект с последующим контролем выполнения и оценкой эффективности принятых решений (корректировкой).

Поддержка принятия решения – это совокупность процедур по обеспечению специалиста по информационной безопасности необходимой информацией и повышение объективности принятия решения в стрессовой ситуации. Показателем эффективности является вероятность своевременного принятия и реализации правильного решения. Так, согласно [6], в качестве показателя эффективности целесообразно выбирать вероятность своевременного принятия и реализации правильного решения, обеспечивающего оптимальное использование наличных ресурсов и средств.

---

[7] Рекомендации по структуре и содержанию плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности кредитной организации в случае возникновения нестандартных и чрезвычайных ситуаций, а также по организации проверки возможности его выполнения (Приложение 5 к Положению Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»).

[8] ГОСТ Р ИСО/МЭК 27031-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. М.: Стандартинформ, 2014. 33 с.

[9] ГОСТ Р МЭК 62508-2014. Национальный стандарт Российской Федерации. Менеджмент риска. Анализ влияния на надежность человеческого фактора. М.: Стандартинформ, 2015. 48 с.

Материалы и методы исследования

Общая схема процесса принятия управленческих решений специалистом по информационной безопасности при реагировании на компьютерный инцидент с использованием СППР состоит из последовательности этапов, к которым можно отнести: выявление проблем и поиск возможных решений, определение информационной потребности для разрешения проблем, определение критериев и ограничений для принятия управленческих решений (включающих в себя выбор целевых и независимых переменных, установление зависимостей между ними, определение используемых моделей), построение альтернативных вариантов решений проблемы, принятие решения с учетом установленных критериев и ограничений [7].

Выдвинем гипотезу, что квалификация исполнителя оказывает существенное влияние на возможность реализации мероприятий Плана в установленные сроки. Под квалификацией исполнителя понимается совокупная функция, зависящая от уровня образования (знание), опыта проведенных тренировок (закрепленный навык), опыта устранения реальных компьютерных инцидентов (практический навык) и периода, прошедшего с момента последней тренировки (деградация навыка).

Для большинства организаций проблема по обеспечению процесса управления уязвимостями кадровыми, а также техническими ресурсами достаточно актуальна [8]. Задача расчета трудозатрат и необходимой численности персонала в рамках выполнения этапа «Реагирование на компьютерный инцидент» достаточно формализована и единообразна по разным сферам деятельности, так как решается субъектами КИИ на основании руководящих документов Министерства труда и социального развития Российской Федерации[10].

Таким образом, численность персонала Чн, задействованного в реализации мероприятий Плана, определяется по формуле:

$$\text{Чн} = \text{Чсп} \cdot \text{Кн},$$

где Чсп – рассчитанная численность подразделения информационных технологий (информационной безопасности); Кн – коэффициент невыхода на работу, исходя из трудозатрат.

К сожалению, в вышеприведенных формализованных расчетах не учитывается пиковая нагрузка, вызванная компьютерной атакой. Численность подразделения считается исходя из годовых трудозатрат, т. е. объема работ, равномерно распределенного в течение длительного времени.

Формально К_н – коэффициент, учитывающий планируемые невыходы работника во время отпуска, болезни и т. п., определяется выражением:

$$\text{К\_н} = 1 + (\%\ \text{планируемых невыходов на работу})/100,$$

[10] Типовые нормы времени на техническое и сервисное обслуживание информационных ресурсов в государственных (муниципальных) учреждениях (утв. ФГБУ НИИ труда и социального страхования Министерства труда и социальной защиты Российской Федерации 07.03.2014).

где % планируемых невыходов на работу устанавливается по данным бухгалтерского учета организации[11].

Принимая отпуск в 28 календарных дней (31 календарный день при ненормированном рабочем дне), обязательное повышение квалификации раз в три года с длительностью программы обучения не менее 72 часов[12], получаем от 29 до 32 календарных дней в год гарантированного отсутствия основного исполнителя в момент потенциальной реализации мероприятий Плана (проведение нарушителем успешной компьютерной атаки). Так как период недоступности основного исполнителя достаточно существенный, то на время его отсутствия назначается резервный исполнитель. При подготовке целенаправленной компьютерной атаки на субъект КИИ нарушитель имеет возможности выявить личность специалиста безопасности и период его отсутствия (через социальные сети). При этом действующими требованиями по информационной безопасности не предусмотрено корректировок Плана и оценки влияния квалификации резервного исполнителя на время выполнения мероприятий Плана: считается, что квалификация исполнителей одинаковая.

С целью проверки гипотезы о влиянии квалификации исполнителя на ликвидацию последствий компьютерных атак были проведены экспериментальные исследования, в ходе которых задействовались силы безопасности 54 субъектов КИИ, осуществляющих свою деятельность в сферах транспорта и здравоохранения. Эксперимент проводился в течение 2024 года в форме двух тренировок по отработке Плана, разработанного в каждой организации на основании единого методического документа Национального координационного центра по компьютерным инцидентам (НКЦКИ)[13].

Экспериментальное исследование № 1

Цель эксперимента: исследовать влияние квалификации исполнителя на время выполнения типового этапа Плана.

Условия эксперимента: в каждом Плане присутствует обязательный этап – направление информации о компьютерном инциденте в НКЦКИ, – реализуемый путем заполнения карточки регистрации компьютерного инцидента. Он является типовым, единообразным, имеет малую длительность (5 мин) и выполняется одновременно основным и резервным исполнителем в разных помещениях. Время фиксируется с точностью до 0,1 мин (6 с).

[11] Методические рекомендации по формированию службы информационных технологий в медицинских организациях (утв. ФГБУ ЦНИИОИЗ Минздрава России 04.03.2022).

[12] Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

[13] Методические рекомендации по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации. М.: НКЦКИ, 2020.

Поскольку сценарий тренировки единый для всех организаций, а перечень передаваемых сведений (объем и состав) централизовано задан НКЦКИ[14], то время заполнения карточки регистрации компьютерного инцидента определяется исключительно навыком (квалификацией) исполнителя. Иными факторами в рамках данного эксперимента можно пренебречь в силу их незначительного влияния. Превышение планового времени выполнения этапа (5 мин) не прекращает эксперимент, отсчет времени продолжается. В случае грубых ошибок при заполнении карточки регистрации компьютерного инцидента фиксируется неспособность (неподготовленность) исполнителя. Результаты эксперимента № 1 приведены на графике (рисунок 1).

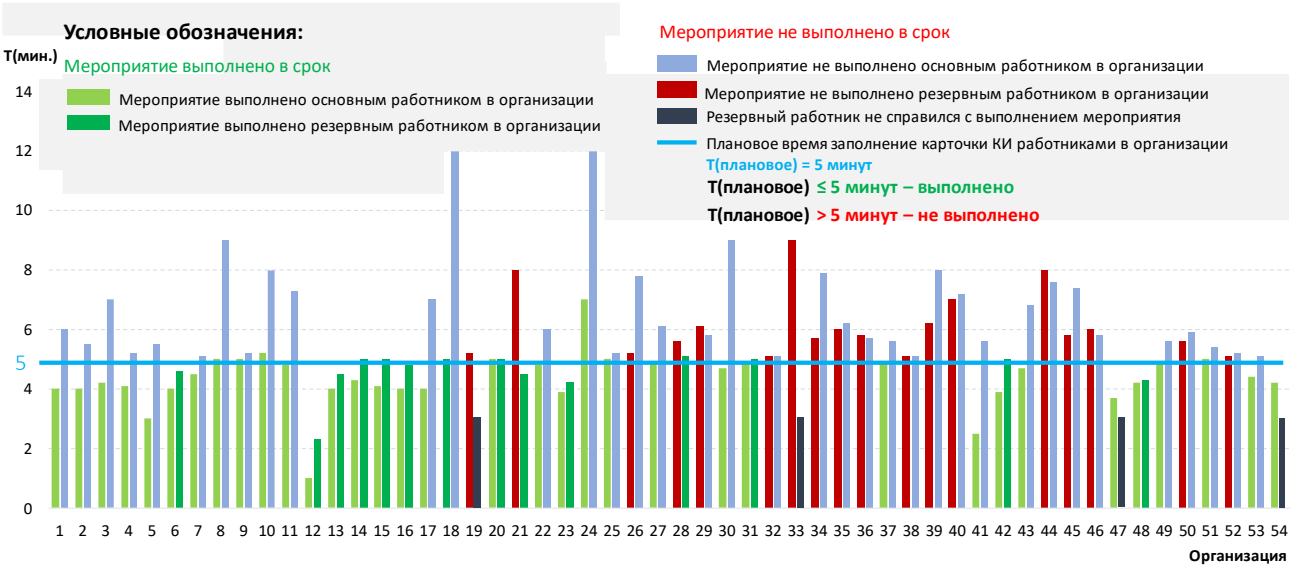

Рис. 1. Разница во времени выполнения одного мероприятия основным и резервным работником по организациям

Видно, что в четырех организациях (7 %) резервные исполнители не имеют должной квалификации для выполнения таких мероприятий. В организации № 21 резервный исполнитель имеет значительно более высокую квалификацию, чем основной. В 14 организациях (26 %) резервный исполнитель тратит на выполнение мероприятия в 1,5 раза больше времени. Только в 11 организациях (20 %) основной исполнитель превысил плановое время, при этом резервные исполнители превысили плановое время в 36 организациях (67 %). Это позволяет сделать вывод о том, что в исследуемой группе 74 % организаций имеют резервных исполнителей с недостаточной квалификацией.

Для проверки гипотезы более важным показателем будет разница во времени выполнения этапа основным и резервным исполнителем. Отразим эту разницу на графике выполнения типового этапа (рисунок 2).

[14] Инструкция по формированию электронного письма уведомления о компьютерном инциденте или атаке. М., 2023.

DOI: 10.31854/2307-1303-2025-13-4-15-30
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2025_4/15-30.pdf

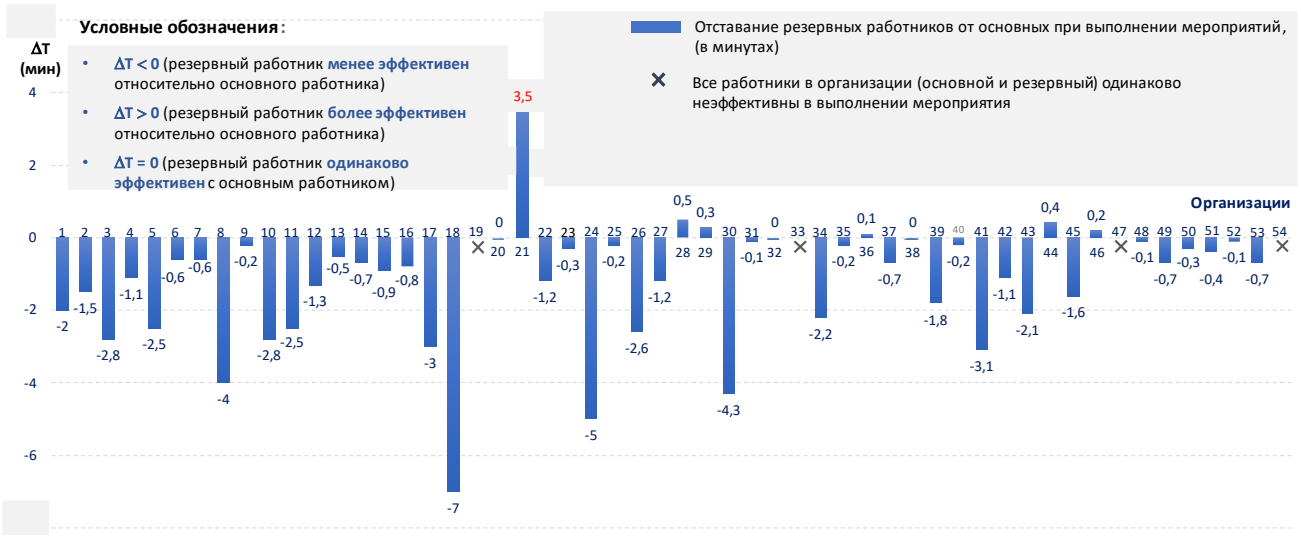

Рис. 2. Анализ разницы времени выполнения мероприятия основным и резервным работником

С учетом погрешностей измерений допустимо считать, что в 21 организации (39 %) обеспечен идентичный уровень квалификации исполнителей.

Экспериментальное исследование № 2

Цель эксперимента: исследовать влияние квалификации исполнителя на эффективность аварийно-восстановительных работ.

Условия эксперимента: каждая организация проводит две тренировки с интервалом в 6 месяцев и с одинаковым сценарием. Первую тренировку проводит основной исполнитель, вторую – резервный. Для исполнителей замена является неожиданной, посредник доводит вводную о замене на резервного исполнителя после начала тренировки. Время фиксируется с точностью до минуты. Если время реализации Плана превысило установленное время тренировки (120 мин), то фиксируется невыполнение Плана и эксперимент в данной организации прекращается.

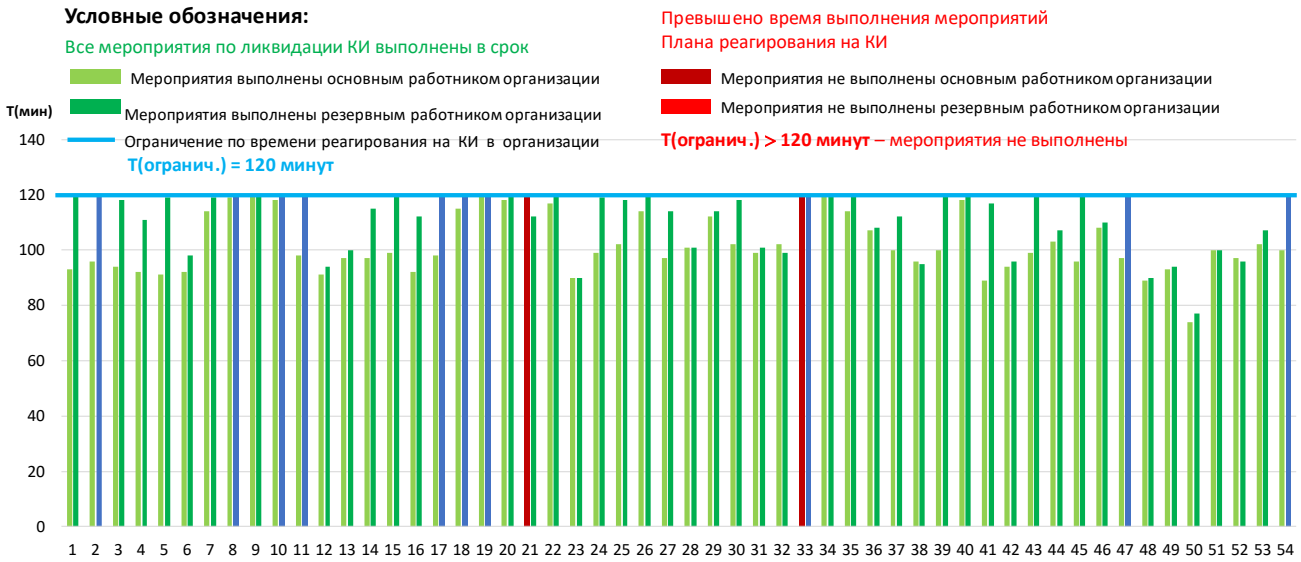

Рис. 3. Оценка эффективности основных и резервных работников при реагировании на компьютерный инцидент

DOI: 10.31854/2307-1303-2025-13-4-15-30
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2025_4/15-30.pdf

Результаты данного эксперимента приведены на графике (рисунок 3): они более «загрязнены» субъективными факторами, которые оказывают существенное влияние на время реализации Плана в конкретной организации. Разница во времени выполнения Плана отражена на рисунке 4.

Рис. 4. Сравнение времени, затраченного основным и резервным работником на выполнение мероприятий плана реагирования на компьютерный инцидент в организации

Наглядно показано, что в 10 организациях (18,5 %) резервный исполнитель не смог заменить основного при проведении тренировки. Еще в 11 организациях (20 %) квалификация резервного исполнителя позволила реализовать План, но за счет превышения затрат времени на 10 %.

Таким образом, можем считать выдвинутую гипотезу доказанной. Соответственно, для решения задачи назначения исполнителя на каждое мероприятие Плана необходимо провести оценку квалификации и соотнести ее с минимально необходимой для реализации в заданные сроки.

Методы исследования человеческой надежности используются для системной оценки воздействия ошибок обслуживающего персонала на устойчивое функционирование объектов КИИ. При использовании метода оценки и сокращения человеческих ошибок учитываются условия, приводящие к возникновению ошибки исполнителя Плана: «несоответствие уровня обучения персонала требованиям задачи» с весовым показателем «2», «неопытность, при наличии необходимой квалификации» с весовым показателем «3», «неизвестная ситуация, редко происходящая», с весовым показателем «17» [9]. Таким образом, допустимо сделать вывод: надежность исполнителя мероприятия Плана достигается после накопления определенного опыта (количества проведенных тренировок) и поддержания его (регулярность тренировок). С точки зрения обеспечения безопасности КИИ, выполнение мероприятия Плана необходимо осуществлять не только в заданные сроки, но и безошибочно.

DOI: 10.31854/2307-1303-2025-13-4-15-30
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2025_4/15-30.pdf

В соответствии с методом когнитивной надежности человека, используемым при анализе задач, решение которых не требуют от исполнителя делать выбор предпринимаемых действий (возможность совершения ошибки при оценке ситуации ограничена, определен единственный (плановый) способ выполнения аварийно-восстановительной операции (мероприятия)), вероятность ошибки исполнителя относительно времени выполнения конкретного мероприятия Плана зависит от типа действий исполнителя: основанных на знаниях (A_i), правилах (B_i) и навыке (C_i).

С учетом влияния времени выполнения мероприятия Плана используем формулу:

$$P = \exp\left\{-\left[\frac{t/T_{1/2}-B_i}{A_i}\right]^{C_i}\right\},$$

где P – вероятность ошибки для отведенного на выполнение времени; t – фактически отведенное время на выполнение мероприятия Плана; $T_{1/2}$ – уточненное среднее время выполнения мероприятия Плана; A_i, B_i, C_i – коэффициенты, связанные с преобладающим типом действий исполнителя [10].

Как показано в исследовании [11], кроме процесса приобретения навыков целесообразно учесть процесс утраты навыков, предполагающий возможность их восстановления. Каждая тренировка снижает частоту ошибок до некоторого уровня, а за время отсутствия тренировок происходит утрата навыка до критического уровня.

Введем систему оценки любого потенциального исполнителя по каждому мероприятию Плана, для чего необходимо задать пороговое значение квалификации, минимально необходимое для его выполнения (таблица 1). Отметим, что веса показателей могут отличаться для конкретных мероприятий Плана. В отдельных случаях важнее практический опыт (закрепленный навык), в других – образованность, позволяющая принимать адекватные решения в условиях неопределенности развития аварийной ситуации (компьютерного инцидента) [12].

Таблица 1. Пороговые значения показателей квалификации

Мероприятие Плана	Образованность, оценки	Вес	Общий стаж, лет	Вес	Опыт реагирования, количество тренировок	Вес
1	4	0,3	1	0,2	0	0
2	5	1	3	0,75	2	1
3	4	0,5	1	0,4	2	0,75
…..						
N	0	0	5	1	2	1

Результаты оценки будут соотносится с четырьмя типами решения: тип 1 – приоритетное назначение, тип 2 – возможное назначение; тип 3 – нежелательное назначение; тип 4 – назначение запрещено. Полученный массив данных для загрузки в СППР приведен в таблице 2.

Таблица 2. База данных исполнителей с типом решения о назначении

Мероприятие Плана	Исполнитель 1	Исполнитель 2	….	Исполнитель М
1	1	1	….	1
2	4	3	….	3
….	….	….	….	…..
N	2	2	….	2

Результаты исследования и их обсуждение

Необходимо отметить, что в соответствии с требованиями приказов ФСБ России субъекты КИИ проводят тренировки по отработке Плана, а не по реагированию на компьютерный инцидент. Таким образом, если субъект КИИ разработал План для формального выполнения требований законодательства, а реагирование на компьютерные инциденты и ликвидация последствий компьютерных атак будет проводиться по иным практикам, то полученные экспериментальные данные могут потребовать уточнения.

Пусть задан полный ориентированный двудольный граф $G = (Q, A)$, где $Q \in Qi$ – исполнители, $A \in Ai$ – мероприятия Плана, каждое ребро графа характеризует вероятность своевременного безошибочного выполнения работ исполнителями Qi мероприятий Плана Ai.

Возникает задача поиска максимального паросочетания в заданном двудольном графе, для решения которой предлагается использовать венгерский алгоритм. С учетом наличия неопределенностей большой интерес представляет теория нечетких множеств (моделей нечеткого графа) [13], которая уже нашла широкое применение при решении научных задач в области информационной безопасности [14, 15]. Определенный опыт накоплен в транспортной сфере и химической промышленности [16, 17]. Использование нейронечеткого модуля расчета оптимального распределения исполнителей в СППР в перспективе позволит снизить число ошибок, обусловленных человеческим фактором в стрессовой ситуации [18]. Вполне целесообразно дополнительно рассмотреть возможность адаптации к решаемым задачам динамических моделей систем принятия решений МЧС России [19, 20].

Заключение

В настоящей статье предложено рассматривать эффективность назначения исполнителя для выполнения Плана по расчетному времени, с учетом основных показателей квалификации и навыков. В работе использованы результаты экспериментальных исследований (объем выборки – более 100 респондентов). Предложенный подход может применяться при актуализации методических и руководящих документов по информационной безопасности, включая устранение уязвимостей программных и программно-аппаратных средств значимых объектов КИИ, и при планировании действий в нештатных ситуациях, не вызванных компьютерными атаками.

DOI: 10.31854/2307-1303-2025-13-4-15-30
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2025_4/15-30.pdf

В дальнейшем планируется уточнение модели исполнителя за счет включения новых параметров и введения интервальных весов показателей [21], что позволит более достоверно оценивать эффективность проведения мероприятий по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак. Для практического применения разрабатывается программное обеспечение СППР специалиста информационной безопасности. Кроме того, проводится работа по анализу возможностей применения полученной модели для решения смежных задач информационной безопасности – устранения уязвимостей, аварийно-восстановительных работ, нештатных ситуаций.

Литература

1. Талашманова К. А. К проблеме понимания профессиональной надежности субъекта // Человеческий капитал. 2020. № 3 (135). С. 239–245. DOI: 10.25629/HC.2020.03.28. DOI: 10.25629/HC.2020.03.28. EDN: TQLYSF

2. Табакаева В. А., Карманов И. Н., Ан В. Р. Особенности интеллектуальных систем управления информационной безопасностью объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2020. Т. 6. № 2. С. 99–104. DOI: 10.33764/2618-981X-2020-6-2-99-104. EDN: AVQHQD

3. Васильев Н. П., Скворцов Р. Р. Использование системы принятия решений для обеспечения информационной безопасности // Актуальные исследования. 2023. № 24-1 (154). С. 43–49. EDN: DHBWDY

4. Фисун В. В. Экспертная система поддержки и принятия решений по управлению информационной безопасностью объектов критической информационной инфраструктуры // Globus: Технические науки. 2022. Т. 8. № 1 (42). С. 17–21. DOI: 10.52013/2713-3079-42-1-4. EDN: IZALNY

5. Хранилов В. П., Бураго П. Н. Математическое обеспечение системы поддержи принятия решений для управления рисками информационной безопасности // Математические методы в технологиях и технике. 2024. № 6. С. 107–110. EDN: DZQSPY

6. Голдобина А. С., Исаева Ю. А., Селифанов В. В., Климова А. М., Зенкин П. С. Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21. № 4. С. 51–58. DOI: 10.21293/1818-0442-2018-21-4-51-58. EDN: YYSUPZ

7. Медведев Д. В., Матвеев А. В. Алгоритмы интеллектуальной поддержки принятия управленческих решений при угрозах лесных пожаров // Научно-аналитический журнал «Вестник Санкт-Петербургского университета ГПС МЧС России». 2025. № 2. С. 35–48. DOI: 10.61260/2218-13X-2025-2-35-48. EDN: OKGHLE

8. Микиденко Н. Л., Сторожева С. П., Струкова Е. Г. Кадровое обеспечение образовательных программ в области информационной безопасности: проблемы проектирования и развития // Вестник СибГУТИ. 2022. 3 (59). С. 84–100. DOI: 10.55648/1998-6920-2022-16-3-84-100. EDN: INPJMX

9. Ахмеджанов Ф. М., Крымский В. Г. Алгоритм оценки надежности человека-оператора на основе модифицированной методики HEART // Электротехнические и информационные комплексы и системы. 2019. Т. 15. № 1. С. 60–69. DOI: 10.17122/1999-5458-2019-15-1-60-69. EDN: PNGLWR

10. Берберова М. А., Чуенко В. В., Золотарев О. В., Андреев В. В., Карпушин Е. В. и др. Оценка действий персонала при наиболее опасных авариях. Разработка программы мониторинга обеспечения безопасности АЭС // Автоматизация и моделирование в проектировании и управлении. 2020. № 2 (8). С. 42–49. DOI: 10.30987/2658-6436-2020-2-42-49. EDN: SIBZER

11. Кондратьев А. Ю., Коваленко О. В., Усов А. В., Ерошкина И. В. Методика оценки вероятности ошибочных действий персонала структурных подразделений Министерства обороны Российской Федерации, эксплуатирующих ядерно и радиационно опасные объекты // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2022. № 7–8 (169–170). С. 3–11. EDN: OFZQAH

12. Ковальковская Н. О., Кулешов В. В., Сердюк В. С., Бакико Е. В. Шкалирование параметров влияния человеческого фактора на уровень профессионального риска на объектах машиностроения // Омский научный вестник. 2020. № 6 (174). С. 15–21. DOI: 10.25206/1813-8225-2020-174-15-21. EDN: GYSRHG

13. Сперанский Д. В. Поиск оптимальных путей в нечетких графах // Автоматика на транспорте. 2022. Т. 8. № 4. С. 418–426. DOI: 10.20295/2412-9186-2022-8-04-418-426. EDN: DEACCM

14. Большаков А. С., Жила А. И., Осин А. В. Управление информационной безопасностью персональных данных с использованием нечеткой логики // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 4. С. 37–47. DOI: 10.36724/2409-5419-2021-13-4-37-47. EDN: AGYPHZ

15. Рябова В. А. Нечеткая модель угроз информационной безопасности предприятия // Молодежная наука – 2023: технологии и инновации: материалы Всероссийской научно-практической конференции молодых ученых, аспирантов и студентов, посвященной Десятилетию науки и технологий в Российской Федерации (10–14 апреля 2023 г., Пермь). Пермь, 2023. С. 103–106. EDN: KGHWKN

16. Carlos Eduardo Rodriguez. Evaluating the impact of human factors on aircraft maintenance errors: A risk-based analysis framework for business aviation. World Journal of Advanced Engineering Technology and Sciences, 2024, 13(02), 764-777. DOI: https://doi.org/10.30574/wjaets.2024.13.2.0647.

17. Zarei E., Khan F., Abbassi R. Importance of Human Reliability in Process Operation: A Critical Analysis // Reliability Engineering & System Safety. 2021. Vol. 211. P. 107607. DOI: 10.1016/j.ress.2021.107607. EDN: EWNXCL

18. Гончарова Н. А. Метод нахождения динамических приоритетов грузовых операций для оптимизации работы самоходных подвижных единиц в железнодорожных промышленных транспортно-технологических системах // Автоматика на транспорте. 2023. Т. 9. № 3. С. 274–282. DOI: 10.20295/2412-9186-2023-9-03-274-282. EDN: DIKMUC

19. Журавлев Н. М. Алгоритм принятия управленческих решений для руководителя тушения пожара в условиях неопределенности // Инновационные иссле-

дования как локомотив развития современной науки: от теоретических парадигм к практике: электронный сборник научных статей по материалам XIII Международной научно-практической конференции (12 октября 2019 г., Москва). М.: НИЦ МИСИ, 2019. С. 193–196.

20. Журавлев Н. М. Поддержка принятия решения руководителя тушения пожара на основе системно-динамической модели фронтального тушения пожара // Приоритетные направления развития Российской науки: материалы IV всероссийской научно-практической конференции (14 июля 2020 г., Санкт-Петербург). СПб., 2020. С. 17–21. EDN: VXJJDZ

21. Крымский В. Г., Ахмеджанов Ф. М. Использование интервальных моделей неопределенностей для оценки надежности человека-оператора с помощью метода SLIM // Электротехнические и информационные комплексы и системы. 2022. Т. 18. № 2. С. 128–138. DOI: 10.17122/1999-5458-2022-18-2-128-138. EDN: IHMGQL

Статья поступила 28 ноября 2025 г.
Одобрена после рецензирования 20 декабря 2025 г.
Принята к публикации 21 декабря 2025 г.

Информация об авторе

Комаров Валерий Валерьевич – старший преподаватель кафедры информационных систем и технологий в здравоохранении Научно-исследовательского института организации здравоохранения и медицинского менеджмента Департамента здравоохранения города Москвы. E-mail: Vinnipux1@rambler.ru

https://doi.org/10.31854/2307-1303-2025-13-4-15-30
EDN: TTTFWO

A Methodological Approach to Determining the Reliability of the Executor of the Computer Incident Response Plan at Significant Facilities of Critical Information Infrastructure

V. Komarov

Moscow Research Institute of Healthcare Organization and Medical Management of the Moscow Health Department, Moscow, 115088, Russian Federation

The purpose *of the study is to determine the reliability of an employee of a critical information infrastructure entity involved in implementing measures to respond to computer incidents and eliminate the consequences of computer attacks on significant objects of the specified infrastructure, as well as to assess the feasibility of using this parameter to characterize the employee in decision support systems. As* ***part of the solution to the problem*** *of assigning responsible employees to implement measures to respond to computer incidents and eliminate the consequences of computer attacks,* ***a methodological approach*** *has been proposed to determine the reliability of the employee responsible for implementing the computer incident response plan. Practical experimental studies have been conducted to assess the effectiveness of the actions of employees of critical information infrastructure entities with different qualifications and skills.* ***As a result*** *of the study, an approach is proposed to calculate the main indicators of the performer's qualifications and skills, as well as to use the obtained indicators when solving the task of assigning performers (the assignment problem), which will reduce the time required to respond to a computer incident and eliminate the consequences of a computer attack. The obtained results allow for the reasonable formation of requirements for the qualifications and skills of personnel in the security forces of significant critical information infrastructure facilities and ensure the interchangeability of performers.* ***The practical significance*** *lies in solving the problem of optimal distribution (assignment) of an executor, taking into account their qualifications and skills, when responding to computer incidents and eliminating the consequences of computer attacks.*

Key words: *critical information infrastructure, object of critical information infrastructure, computer incident, model, computer attack*

References

1. Talashmanova K. A. To the Problem of Understanding the Professional Reliability of a Subject // Chelovecheskij Kapital. 2020. Iss. № 3 (135). PP. 239–245. (in Russian) DOI: 10.25629/HC.2020.03.28. EDN: TQLYSF

2. Tabakaeva V. A., Karmanov I. N., An V. R. Features of Intelligent Information Security Management Systems for Critical Information Infrastructure Objects // Interexpo Geo-Siberia. 2020. Vol. 6. Iss. 2. PP. 99–104. (in Russian) DOI: 10.33764/2618-981X-2020-6-2-99-104.EDN: AVQHQD

3. Vasiliev N. P., Skvortsov R. R. Using a Decision-Making System to Ensure Information Security // Current Research. 2023. Iss. 24–1 (154). Ч. I. PP. 43–49. (in Russian) EDN: DHBWDY

4. Fisun V. V. Expert System for Support and Decision-Making on the Management of Information Security of Objects of Critical Information Infrastructure // Globus: Technical Sciences. 2022. Vol. 8. Iss. 1 (42). PP. 17–21. (in Russian) DOI: 10.52013/2713-3079-42-1-4. EDN: IZALNY

5. Khranilov V. P., Burago P. N. Mathematical Support of a Decision Support System for Information Security Risk Management Purposes // Mathematical Methods in Technologies and Technics. 2024. Iss. 6. PP. 107–110. (in Russian) EDN: DZQSPY

6. Goldobina A. S., Isaeva Ju. A., Selifanov V. V., Klimova A. M., Zenkin P. S. Building an Adaptive Three-Tier Model of Management Processes for the Information Security System of Critical Information Infrastructure Objects // Proceedings of the TUSUR University. 2018. Vol. 21. Iss. 4. PP. 51–58. (in Russian) DOI: 10.21293/1818-0442-2018-21-4-51-58. EDN: YYSUPZ

7. Medvedev D., Matveev A. Algorithms for Intelligent Support of Management Decisions in Case of Threats from Forest Fires // Scientific and Analytical Journal "Vestnik Saint-Petersburg University of State Fire Service of Emercom of Russia". 2025. № 2. С. 35–48. (in Russian) DOI: 10.61260/2218-13X-2025-2-35-48. EDN: OKGHLE

8. Mikidenko N. L., Storozheva S. P., Strukova E. G. Staff Assistance of Educational Programs in the Sphere of Information Security: Design and Development Problems // Vestnik SibGUTI. 2022. Iss. 3 (59). PP. 84–100. (in Russian) DOI: 10.55648/1998-6920-2022-16-3-84-100. EDN: INPJMX

9. Akhmedzhanov F. M., Krymsky V. G. HEART Algorithm for Assessment of Human Operator Reliability Based on Modified Heart Methodology // Electrical Engineering and Information Complexes and Systems. 2019. Vol. 15. Iss. 1. PP. 60–69. (in Russian) DOI: 10.17122/1999-5458-2019-15-1-60-69. EDN: PNGLWR

10. Berberova M., Chuenko V., Zolotarev O., Andreev V., Karpushin E., et al. Assessment of Personnel Actions in the Most Dangerous Accidents. Development of a NPP Safety Monitoring Program // Automation and Modeling in Design and Management. 2020. Iss. 2 (8). PP. 42–49. (in Russian) DOI: 10.30987/2658-6436-2020-2-42-49. EDN: SIBZER

11. Kondratyev A. Yu., Kovalenko O. V., Usov A. V., Eroshkina I. V. Methodological Approach for Assessing the Risks of Erroneous Actions of Personnel Structural Divisions of the Ministry of Defense of the Russian Federation, Operating Nuclear and Radiation Hazardous Facilities // Defense Technology Issues. Series 16: Technical Means of Countering Terrorism. 2022. Iss. 7–8 (169–170). PP. 3–11. (in Russian) EDN: OFZQAH

12. Kovalkovskaya N. O., Kuleshov V. V., Serdyuk V. S., Bakiko E. V. Human Factor Parameters Influence Scaling on Professional Risk Level at Engineering Facilities // Omsk Scientific Bulletin. 2020. Iss. 6 (174). PP. 15–21. (in Russian) DOI: 10.25206/1813-8225-2020-174-15-21. EDN: GYSRHG

13. Speranskiy D. About Search of Optimal Paths in Fuzzy Graphs // Automation in Transport. 2022. Vol. 8. Iss. 4. PP. 418–426. (in Russian) DOI: 10.20295/2412-9186-2022-8-04-418-426. EDN: DEACCM

14. Bolshakov A. S., Zhila A. I., Osin A. V. Fuzzy Logic Data Protection Management // High Technologies in Earth Space Research. 2021. Vol. 13. Iss. 4. PP. 37–47. (in Russian) DOI: 10.36724/2409-5419-2021-13-4-37-47. EDN: AGYPHZ

15. Ryabova V. A. Fuzzy Model of Enterprise Information Security Threats // Proceedings of the All-Russian Scientific and Practical Conference of Young Scientists, Postgraduates and Students, Dedicated to the Decade of Science and Technology

in the Russian Federation “Youth Science – 2023: Technologies and Innovations” (April 10–14, 2023, Perm). Perm, 2023. PP. 103–106. EDN: KGHWKN (in Russian)

16. Carlos Eduardo Rodriguez. Evaluating the impact of human factors on aircraft maintenance errors: A risk-based analysis framework for business aviation. World Journal of Advanced Engineering Technology and Sciences, 2024, 13(02), 764-777. DOI: https://doi.org/10.30574/wjaets.2024.13.2.0647.

17. Zarei E., Khan F., Abbassi R. Importance of Human Reliability in Process Operation: A Critical Analysis // Reliability Engineering & System Safety. 2021. Vol. 211. P. 107607. DOI: 10.1016/j.ress.2021.107607. EDN: EWNXCL

18. Goncharova N. Method for Determining Dynamic Priorities of Cargo Operations for Optimizing the Use of Self-Propelled Units in Railway Industrial Transport and Technological Systems // Automation in Transport. 2023. Vol. 9. Iss. 3. PP. 274–282. (in Russian) DOI: 10.20295/2412-9186-2023-9-03-274-282. EDN: DIKMUC

19. Zhuravlev N. M. Decision-Making Algorithm for a Firefighting Command Officer under Uncertainty // Innovative Research as a Locomotive for the Development of Modern Science: From Theoretical Paradigms to Practice: Electronic Collection of Scientific Articles Based on the XIII International Scientific and Practical Conference Materials (October 12, 2019, Moscow). Moscow: MISI University Publ., 2019. PP. 193–196. (in Russian)

20. Zhuravlev N. M. Support Decision-Making of Head of Fire Extinguishing Based on System-Dynamic Models Frontal Fire Fighting // Proceedings of the IV All-Russian Scientific and Practical Conference on Priority Areas for the Development of Russian Science (July 14, 2020, St. Petersburg). St. Petersburg, 2020. PP. 17–21. (in Russian) EDN: VXJJDZ

21. Krymsky V., Akhmedzanov F. Application of Interval Models of Uncertainties to Assessing Human Operator Reliability by SLIM Method // Electrical Engineering and Information Complexes and Systems. 2022. Vol. 18. Iss. 2. PP. 128–138. (in Russian) DOI: 10.17122/1999-5458-2022-18-2-128-138. EDN: IHMGQL

Information about Author

Komarov Valery – Senior Lecturer at the Department of Information Systems and Technologies in Healthcare (Moscow Research Institute of Healthcare Organization and Medical Management of the Moscow Health Department).
E-mail: Vinnipux1@rambler.ru