Метод оптимизации организационной структуры и функционала сотрудников подразделения по защите информации, обслуживающего автоматизированную систему в защищенном исполнении

А.Д. Трофимович

РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва

Аннотация: Целью исследования является разработка решения, позволяющего оптимизировать численность и функционал специалистов подразделения по защите информации, участвующих в обеспечении информационной безопасности автоматизированной системы в защищённом исполнении. В работе анализируются существующие требования к персоналу, обслуживающему автоматизированную систему в защищенном исполнении, их функционалу и выполняемым трудовым действиям и выявляются недостатки действующих нормативно-методических документов, описывающих функционал персонала, обеспечивающего защиту информации объекта. Предлагается решение по оптимизации численности и функционала специалистов, участвующих в обеспечении информационной безопасности организации. Оно подчёркивает важность повышения квалификации и унификации компетенций работников информационной безопасности для обеспечения их взаимозаменяемости и снижения различных рисков, что позволит повысить устойчивость и эффективность системы защиты информации на предприятии.

Ключевые слова: Информационная безопасность, администратор, штатная численность, функционал персонала информационной безопасности, автоматизированная система в защищенном исполнении.

Как известно, обеспечение информационной безопасности (далее ИБ) крайне важно для любой организации, которая работает со сведениями ограниченного доступа.

Разработкой требований по безопасности информации, циркулирующей в автоматизированных системах организации, занимается, в том числе, Федеральная служба по техническому и экспортному контролю России, которая выпустила руководящие Приказы №17 (Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" // Официальный сайт Федеральной службы по техническому и экспортному контролю. URL: fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-

2013-g-n-17?ysclid=mhnu4wo9w1625032675), № 21 (Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" // Официальный сайт Федеральной службы по техническому и экспортному контролю. URL: fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21?ysclid=mhnu4gjs7g182687367) и № 239 (Приказ ФСТЭК России от 25.12.2017 № 239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры" // Официальный интернет-портал правовой информации. URL: publication.pravo.gov.ru/document/0001201803270041).

Тем не менее, следует помнить, что обеспечение работоспособности и надёжности системы защиты информации на предприятии невозможно без наличия квалифицированного персонала, обслуживающего систему, для которой необходимо обеспечить безопасность обрабатываемых в ней данных. Перечень необходимых должностей работников определены Госстандартом (Постановление Госстандарта РФ от 26.12.1994 № 367 "О принятии и введении в действие Общероссийского классификатора профессий рабочих, должностей служащих и тарифных разрядов ОК 016-94" (вместе с "ОК 016-94. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов") // Справочно-правовая система Контур. Норматив. URL: normativ.kontur.ru/document?moduleId=1&documentId=122405) и Министерством труда РФ (Приказ Минтруда России от 14.09.2022 г. № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» // Официальный интернет-портал правовой информации. URL:

publication.pravo.gov.ru/Document/View/0001202210170003), а функциональные требования к ним указываются в нормативных документах, утверждённых Приказами Федерального агентства по техническому регулированию и метрологии - ГОСТ Р 53114-2008 (ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. // Информационный портал «Охрана труда в России». URL: ohranatruda.ru/upload/iblock/ea5/4293826768.pdf) и ГОСТ Р ИСО/МЭК 27002-2021 (ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. // Официальный сайт Федерального агентства по техническому регулированию и метрологии. URL: protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=230363).

Для выполнения вышеуказанных требований необходимо большое количество квалифицированных работников подразделения по защите информации, что экономически невыгодно даже для средних, не говоря уже о небольших предприятиях.

Таким образом, целью данного исследования является разработка способа уменьшения расходов организации на обеспечение надежной защиты своих информационных ресурсов.

Необходимые требования к квалификации, функционалу и оптимизации численности персонала организации, а также вопрос повышения производительности труда нашли своё отражение в научных трудах различных авторов. В статье [1], где рассматриваются ключевые проблемы управления персоналом на российских предприятиях, авторы особенно выделяют недостаток мотивации, низкий уровень квалификации сотрудников и слабое использование современных HR-технологий и

предлагают пути улучшения управления для повышения эффективности работы и конкурентоспособности организаций. Публикация Авдеева М.Ю. [2] представляет обзор современных теоретических подходов к управлению производительностью труда, рассматривает методы оценки, мотивации и организации труда, направленные на повышение эффективности работы, также автор анализирует влияние факторов организационной культуры, инноваций и технологий на рост производительности в различных отраслях экономики. В научной публикации [3] рассматривается роль сертификации квалификаций в развитии человеческого капитала и подчеркивается, что сертификация способствует объективной оценке профессиональных навыков, повышению качества труда и конкурентоспособности специалистов, что важно для экономического роста и эффективного управления кадрами.

Сразу несколько научных трудов посвящены оптимизации структуры и численности персонала: статья Суваловой Т.В. [4] анализирует методы оптимизации численности персонала, включая количественные и качественные подходы, рассматривает инструменты оценки эффективности занятости, автоматизацию процессов и применение кадрового планирования и уделяет особое внимание балансу между снижением затрат и сохранением производственной эффективности для устойчивого развития организации; в статье Ильченко С.В. и Андрющенко Н.Ш. [5] рассматриваются методы оптимизации структуры персонала компании в условиях кризиса, анализируются сокращение затрат и повышение эффективности за счёт реструктуризации, переобучения сотрудников и распределения ролей и предлагаются практические рекомендации для адаптации кадровой политики к экономическим вызовам и сохранения стабильности бизнеса; в своём научном труде [6], который посвящен повышению эффективности труда на промышленных предприятиях через оптимизацию штатной численности, Долженко Р.А. и Гусакин А.А. исследуют методы корректировки

численности персонала с учётом производственных требований, что снижает издержки и повышает производительность, одновременно улучшая безопасность и условия труда работников.

Вопросы определения штатной численности подразделения по защите информации также рассматриваются в научных произведениях. Так, в своей статье [7], которая посвящена применению регрессионного моделирования для определения оптимальной штатной численности подразделений по защите информации, авторы разрабатывают математические модели, учитывающие специфические факторы безопасности, что позволяет повысить точность планирования кадров и эффективность работы служб защиты данных. В труде Носкова С.И. и Медведева А.П. [8] проводится анализ укомплектованности подразделений по защите информации в регионах России с помощью регрессионного моделирования, в рамках которого авторы выявляют зависимость численности сотрудников от ключевых факторов, оценивая эффективность распределения кадров и предлагая оптимальные подходы для улучшения безопасности информации.

Несколько научных произведений, в том числе зарубежных авторов, посвящены важнейшей роли персонала в контексте обеспечения ИБ организации. Так, в статье Уразовой К.А. и Дикаревой О.С. [9] рассматривается кадровая безопасность как ключевой элемент системы ИБ нефтегазового комплекса, анализируются угрозы, связанные с персоналом, и предлагаются меры по отбору, обучению и контролю сотрудников для защиты информации и предотвращения внутренних рисков; в труде Гафаровой А.Д. [10] рассматриваются методы организации работы с персоналом для обеспечения ИБ на предприятии и подчеркивается важность обучения сотрудников, разработки внутренних регламентов и контроля доступа, что снижает риски утечек информации и повышает общую защиту информационных систем предприятия; произведение Полякова А.В. [11]

выделяет ключевую роль персонала в обеспечении ИБ организации и подчеркивает необходимость повышения квалификации сотрудников, формирования культуры безопасности и ответственности, поскольку эффективное управление персоналом снижает внутренние угрозы и способствует защите информационных ресурсов компании от различных рисков; статья [12] анализирует ключевые проблемы управления ИБ, включая рост киберугроз, сложности интеграции технологий и человеческий фактор, и выделяет требования к квалификации специалистов, необходимость оптимизации ресурсов и адаптации стратегий для повышения эффективности защиты информации в организациях; в произведении [13] предлагается мультистратегический подход к управлению ИБ в организациях, подчеркивается важность сочетания различных стратегий – проактивных, реактивных и инновационных – для эффективного противодействия современным угрозам и обеспечения устойчивости бизнеса, обсуждается функционал подразделений по защите информации и методы повышения эффективности и продуктивности персонала; в рамках научного труда [14] разрабатывается интегративная модель, объясняющая, почему сотрудники соблюдают политики ИБ, и учитывающая факторы мотивации, восприятия рисков и социальных норм, тем самым показывая, что осведомленность, личные убеждения и организационная поддержка сотрудников влияют на уровень соблюдения правил безопасности.

Задачей исследования является разработка модели структуры и функционала работников подразделения ИБ, позволяющей оптимизировать его численность, с соблюдением требований по защите информации во время эксплуатации автоматизированной системы в защищенном исполнении (далее АСЗИ), без снижения контроля за обеспечением надёжной защиты информационных ресурсов, как в настоящее время, так и на перспективу.

Поставленная задача исследования может быть решена следующими методами:

1. Оптимизация функционала персонала подразделения по защите информации.

Требования к квалификации персонала определены в Профессиональном стандарте «Специалист по защите информации в автоматизированных системах», принятом Приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 525Н (далее Стандарт). В нём указаны не только требования к квалификации персонала, но и перечень должностей специалистов по ИБ, требования к квалификации, необходимые знания и умения работников. Можно отметить, что требования к работникам, связанным с обеспечением ИБ на предприятии отражены всесторонне и охватывают все необходимые функции персонала.

Вместе с тем, многое из перечня трудовых действий, определённых Стандартом, носит разовый или не определённый временными рамками характер и не является критически важным для каждодневного поддержания ИБ на требуемом уровне.

В качестве решения этой проблемы предприятию, вместо набора персонала, необходимо передать на аутсорсинг специализированной организации предусмотренные Стандартом действия, не влияющие на текущее обеспечение безопасности.

Этим предприятие сможет снизить расходы на содержание персонала ИБ, без ухудшения уровня защиты информации в АСЗИ.

2. Изменение штатной численности и функционала работников подразделения по ИБ, обеспечивающих комплексное соблюдение требований по защите информации в АСЗИ.

Установление требований к квалификации персонала и организационной структуре подразделения, занимающегося обслуживанием

АСЗИ, крайне необходимо для поддержания функционирования системы и исключения «человеческого» фактора при недопущении или реагировании на инциденты нарушения ИБ.

В Стандарте указан перечень должностей работников, связанных с обеспечением ИБ предприятия. Это и Инженер по защите информации, и Специалист по защите информации, и Инженер-программист по технической защите информации и т.д. Несмотря на то, что названия этих должностей соответствуют Общероссийскому классификатору профессий рабочих, должностей служащих и тарифных разрядов, объём задач, выполняемых работником на каждой конкретной должности, не определён, и для полноценного обеспечения защиты информации на предприятии, в соответствии с перечнем задач, необходимо привлекать большое количество работников, связанных с защитой информации. Это приводит к увеличению штатной численности подразделения ИБ работниками с уникальным функционалом, часто не взаимозаменяемым.

Вместе с этим повышение квалификации и расширение функционала персонала, обслуживающего систему ИБ, позволит унифицировать компетенции работников ИБ, повысить их взаимозаменяемость и уменьшит риски отсутствия контроля за обеспечением ИБ, в случае, например, увольнения или болезни узкоспециализированного работника.

Также в Стандарте отсутствуют требования к трудовым действиям по контролю и определению ответственных за комплексное обеспечение соблюдения требований ИБ АСЗИ.

Решением этой проблемы может быть внесение изменений в Стандарт с введением новых должностей, объединяющих и консолидирующих необходимый функционал по обеспечению ИБ предприятия.

В Общероссийском классификаторе профессий рабочих, должностей служащих и тарифных разрядов есть профессия Администратор

информационной безопасности вычислительной сети (далее Администратор ИБ), которая не указана в Стандарте, но на работника на этой должности можно возложить ответственность за комплексное обеспечение безопасности АСЗИ - функционал, консолидирующий и проверяющий действия специалистов по защите информации, инженеров по защите информации и т.д.

На Администратора ИБ можно возложить функции по непосредственному, каждодневному обеспечению функционирования АСЗИ.

Также в Общероссийском классификаторе профессий рабочих, должностей служащих и тарифных разрядов есть профессия Администратор вычислительной сети (далее Администратор АСЗИ), которая также не указана в Стандарте. Эта должность подразумевает непосредственный контроль функционирования АСЗИ, в том числе с оперативным устранением возникающих неисправностей для поддержания ИБ на необходимом уровне.

Таким образом, оптимальная организационная структура подразделения ИБ представляется в следующем виде: Руководитель подразделения; Администратор ИБ; Администратор АСЗИ.

Ниже приводятся примерные должностные обязанности и зона ответственности персонала подразделения по защите ИБ.

- Администратор ИБ

В должностные обязанности Администратора ИБ входит:

– участие в разработке и актуализации матрицы доступа (ролевая модель правил разграничения доступа) АСЗИ; определение состава средств защиты информации (далее СрЗИ) в АСЗИ;

– участие в разработке, согласовании и внесении изменений в нормативную документацию, регламентирующую правила и требования по безопасной работе в АСЗИ; периодическая проверка исправности

используемых СрЗИ и правильность их настройки; передача пользователям, допущенным к работе в АСЗИ, уникального идентификатора (имя учётной записи / логин) и первичной парольной информации; проведение периодического инструктажа пользователей по правилам безопасной и корректной работы в АСЗИ;

– предотвращение возможности нарушений требований безопасности информации в АСЗИ, контроль за работой пользователей и администратора АСЗИ;

– участие в проведении расследований инцидентов ИБ;

– участие в проведении и анализе результатов внутренних аудитов ИБ с целью определения выполнения установленных требований по защите информации в АСЗИ, а также выявление возможных улучшений и определение необходимости проведения корректирующих и предупреждающих мероприятий;

– организация учета: состава программно-технических средств АСЗИ (далее ПТС); установленных СрЗИ в АСЗИ; эксплуатационной и технической документации СрЗИ; состава пользователей; выдачи персональных идентификаторов пользователям; распечатанных документов, содержащих сведения конфиденциального характера; инцидентов ИБ; изменения конфигурации АСЗИ;

– хранение контрольных копий лицензионного программного обеспечения СрЗИ, документации на СрЗИ, контроль соответствия контрольных сумм, установленных программных СрЗИ приведённым в документации;

– осуществление непосредственного контроля за внесением изменений в конфигурацию (модификацию) аппаратно-программных средств АСЗИ, установку и настройку программного обеспечения для обработки конфиденциальной информации, СрЗИ;

– оформление Акта об утилизации и уничтожение информации с отчуждаемых носителей информации, в случае его замены или выхода из строя;

– организация фиксации изменений АСЗИ в организационно-распорядительной документации.

Администратор ИБ несёт предусмотренную законодательством Российской Федерации ответственность:

– за ненадлежащее исполнение своих должностных обязанностей;

– за несвоевременное и неполное выполнение указаний и распоряжений непосредственного руководителя и функционального руководителя по направлению безопасности информации, а также приказов и распоряжений вышестоящего руководства;

– за полноту и достоверность данных, собранных в ходе выполнения возложенных обязанностей и предоставленных руководству;

– за непринятие мер при выявлении нарушений безопасности информации в АСЗИ; за качество проводимых работ по обеспечению защиты информации в соответствии с функциональными обязанностями;

– за разглашение сведений, составляющих конфиденциальную информацию АСЗИ, в том числе о применяемых методах и способах защиты информации в АСЗИ;

– за разглашение аутентификационной информации учётных записей пользователей и администратора АСЗИ.

- Администратор АСЗИ

В должностные обязанности администратора АСЗИ входит:

– участие в подготовке предложений по выбору основного состава ПТС, в его обосновании и согласовании с руководителями соответствующих подразделений;

– согласование устанавливаемого программного обеспечения и обновлений на ПТС с руководителем соответствующего подразделения и администратором безопасности информации;

– работы по установке, отладке, опытной проверке и вводу в эксплуатацию ПТС АСЗИ;

– работы по обновлению до новых версий, изменению политик и настроек, установке патчей в сетевой и ИТ-инфраструктуре АСЗИ в соответствии с рекомендациями, полученными от администратора ИБ для устранения уязвимостей, которые могут быть использованы для нанесения компьютерных атак на защищаемые ресурсы АСЗИ;

– работы по обеспечению бесперебойного функционирования и технического обслуживания компьютерных сетей и коммуникационного оборудования АСЗИ; сопровождение системного программного обеспечения ПТС и прикладных программных средств;

– своевременное устранение неисправности, возникающей в процессе эксплуатации ПТС, обслуживание стандартных программ; своевременная замена непригодного периферийного оборудования на резервное; периодический учет ПТС;

– выполнение регламентных работ по синхронизации базы данных;

– хранение контрольных копий лицензионного программного обеспечения;

– установка минимальных прав доступа для пользователей АСЗИ, необходимых им для выполнения своих функциональных обязанностей;

– управление учетными записями пользователей АСЗИ (заведение, активация, корректировка, блокирование и уничтожение);

– консультация пользователей по работе с ПТС в АСЗИ;

– создание документации, отражающей актуальную структуру локальной сети.

Администратор АСЗИ несёт предусмотренную законодательством Российской Федерации ответственность:

– за ненадлежащее исполнение или неисполнение своих должностных обязанностей; за нарушение функционирования локальной сети, серверов и персональных компьютеров вследствие ненадлежащего исполнения своих должностных обязанностей; за ненадлежащее использование ПТС;

– за сохранность принимаемой и регистрируемой информации;

– за соблюдение правил техники безопасности и инструкций по эксплуатации оборудования.

Вывод

Таким образом, создаётся вертикально интегрированная организационная структура в подразделении ИБ, которая позволит обеспечить соблюдение требований по защиты информации во время эксплуатации АСЗИ. Достоинством этой структуры является чёткое разделение зоны ответственности и обязанностей работников подразделения по обеспечению каждодневного обслуживания системы ИБ предприятия. Также преимуществом этой структуры является её универсальность, так как при изменении конфигурации АСЗИ достаточно просто увеличить количество специалистов, с определённым заранее функционалом, без ввода дополнительных должностей.

Литература

1. Ондар Н.Э., Донгак Ч.Г. Проблемы управления персоналом на российских предприятиях // Экономика и социум. 2017. №5-1 (36). URL: cyberleninka.ru/article/n/problemy-upravleniya-personalom-na-rossiyskih-predpriyatiyah.

2. Авдеев М.Ю. Теоретический обзор современных подходов к управлению производительностью труда // Теория и практика общественного развития. 2019. №5 (135). С. 38–41.

3. Скорев М.М. Человеческий капитал сквозь призму сертификации квалификаций // Инженерный вестник Дона, 2013, №1. URL: ivdon.ru/ru/magazine/archive/n1y2013/1513.

4. Сувалова Т.В. Методы и подходы к оптимизации численности персонала. // Управление. 2017. №3. С. 36-40.

5. Ильченко С.В., Андрющенко Н.Ш. Оптимизация структуры персонала компании в условиях кризиса // Бизнес и дизайн ревю. 2023. №2 (30). С. 87-94.

6. Долженко Р.А., Гусакин А.А. Повышение эффективности труда через оптимизацию штатной численности // Охрана труда и техника безопасности на промышленных предприятиях. 2023. №12.

7. Носков С.И., Медведев А.П., Глухов Н.И. Регрессионное моделирование штатной численности подразделений по защите информации // Инженерный вестник Дона, 2024, №6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9283.

8. Носков С.И., Медведев А.П. Анализ укомплектованности подразделений по защите информации в субъектах Российской Федерации на основе регрессионного моделирования // Инженерный вестник Дона, 2024, №12 URL: ivdon.ru/ru/magazine/archive/n12y2024/9716.

9. Уразова К.А., Дикарева О.С. Кадровая безопасность в системе обеспечения информационной безопасности нефтегазового комплекса // Экономика: вчера, сегодня, завтра. 2022. Том 12. № 5А. С. 425-431. DOI: 10.34670/AR.2022.87.87.038.

10. Гафарова А.Д. Организация работы с персоналом при обеспечении информационной безопасности на предприятии // Материалы IX

Международной студенческой научной конференции «Студенческий научный форум». URL: files.scienceforum.ru/pdf/2017/36030.pdf.

11. Поляков А.В. Место и роль персонала в информационной безопасности организации // Социально-гуманитарные знания. 2011. №5. URL: cyberleninka.ru/article/n/mesto-i-rol-personala-v-informatsionnoy-bezopasnosti-organizatsii.

12. Fenz S., Heurix J., Neubauer T., Pechstein F. Current challenges in information security management // Information Management and Computer Security, 2014, Vol. 22, No. 5, pp. 410-427. DOI: 10.1108/IMCS-07-2013-0053.

13. Ahmad A., Maynard S.B., Park S. Information security strategies: Towards an organizational multi-strategy perspective // Journal of Intelligent Manufacturing, 2016, Vol. 27, No. 6, pp. 1143-1154. DOI:10.1007/s10845-012-0683-0.

14. Siponen M., Adam Mahmood M., Pahnila S. Employees' adherence to information security policies: An integrative model // Information and Management, 2014, Vol. 51, No. 3, pp. 395-403. DOI:10.1016/j.im.2013.08.006.

References

1. Ondar N.E., Dongak CH.G. Ekonomika i sotsium. 2017. №5-1 (36). URL: cyberleninka.ru/article/n/problemy-upravleniya-personalom-na-rossiyskih-predpriyatiyah.

2. Avdeyev M.YU. Teoriya i praktika obshchestvennogo razvitiya. 2019. №5 (135). Pp. 38-41.

3. Skorev M.M. Inzhenernyj vestnik Dona. 2013. №1. URL: ivdon.ru/ru/magazine/archive/n1y2013/1513.

4. Suvalova T.V. Upravleniye. 2017. №3. Pp. 36-40.

5. Il′chenko S.V., Andryushchenko N.SH. Biznes i dizayn revyu. 2023. №2 (30). Pp. 87-94.

6. Dolzhenko R.A., Gusakin A.A. Okhrana truda i tekhnika bezopasnosti na promyshlennykh predpriyatiyakh. 2023. №12.

7. Noskov S.I., Medvedev A.P., Glukhov N.I. Inzhenernyj vestnik Dona. 2024. №6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9283.

8. Noskov S.I., Medvedev A.P. Inzhenernyj vestnik Dona. 2024. №12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9716.

9. Urazova K.A., Dikareva O.S. Ekonomika: vchera, segodnya, zavtra. 2022. Vol.12. №5A. pp. 425-431. DOI: 10.34670/AR.2022.87.87.038.

10. Gafarova A.D. Materialy IX Mezhdunarodnoy studencheskoy nauchnoy konferentsii "Studencheskiy nauchnyy forum". URL: files.scienceforum.ru/pdf/2017/36030.pdf.

11. Polyakov A.V. Sotsialno-gumanitarnyye znaniya. 2011. №5. URL: cyberleninka.ru/article/n/mesto-i-rol-personala-v-informatsionnoy-bezopasnosti-organizatsii.

12. Fenz S., Heurix J., Neubauer T., Pechstein F. Information Management and Computer Security, 2014, Vol. 22, No. 5, pp. 410-427. DOI: 10.1108/IMCS-07-2013-0053.

13. Ahmad A., Maynard S.B., Park S. Journal of Intelligent Manufacturing, 2016, Vol. 27, No. 6, pp. 1143-1154. DOI: 10.1007/s10845-012-0683-0.

14. Siponen M., Adam Mahmood M., Pahnila S. Information and Management, 2014, Vol. 51, No. 3, pp. 395-403. DOI:10.1016/j.im.2013.08.006.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 18.11.2025

Дата публикации: 6.01.2026