УДК 330
DOI 10.26118/2782-4586.2024.67.30.022

Востряков Владимир Сергеевич
Московская международная академия

Методология управления инновациями в обеспечении безопасности в экономических информационных системах

Аннотация. В статье рассматриваются ключевые аспекты методологии управления инновациями в контексте обеспечения безопасности экономических информационных систем (ЭИС). Подчеркивается важность интеграции инновационных подходов в систему управления рисками, связанными с информационной безопасностью. Обсуждаются современные методы анализа угроз и разработки стратегий защиты ЭИС, а также роль инновационных технологий в создании эффективных механизмов противодействия киберугрозам. Кроме того, приведены примеры успешной реализации инновационных решений в области защиты информации, которые способствуют повышению надежности и устойчивости ЭИС. Работа направлена на формирование новых теоретических и практических подходов в управлении безопасностью ЭИС через призму инновационного развития.

Ключевые слова: инновации, безопасность, экономические информационные системы, управление рисками, киберугрозы, методология, устойчивость, информационная безопасность, технологии.

Vostryakov Vladimir Sergeevich
Moscow International Academy

Methodology of innovation management in ensuring security in economic information systems

Annotation. The article discusses the key aspects of the innovation management methodology in the context of ensuring the security of economic information systems (EIS). The importance of integrating innovative approaches into the information security risk management system is emphasized. Modern methods of threat analysis and development of EIS protection strategies are discussed, as well as the role of innovative technologies in creating effective mechanisms to counter cyber threats. In addition, examples of successful implementation of innovative solutions in the field of information security, which contribute to improving the reliability and stability of EIS, are given. The work is aimed at the formation of new theoretical and practical approaches in the management of EIS security through the prism of innovative development.

Keywords: innovation, security, economic information systems, risk management, cyber threats, methodology, sustainability, information security, technology.

Современные экономические информационные системы (ЭИС) становятся все более уязвимыми к различным угрозам, как внутреннего, так и внешнего происхождения. Стремительное развитие технологий, таких как облачные вычисления, большие данные и Интернет вещей, открывает новые горизонты для бизнеса, но в то же время создает дополнительные риски для безопасности. Инновации, внедряемые в процессы управления, могут значительно повысить устойчивость ЭИС к киберугрозам. В данной статье предлагается методология управления инновациями, которая поможет организациям адаптироваться к быстро меняющемуся ландшафту безопасности, обеспечивая при этом защиту критически важных данных и финансовых активов.

Раздел 1. Методы управления инновациями в обеспечении безопасности в экономических информационных системах

Важнейшим аспектом обеспечения безопасности в экономических информационных системах является инновационный подход к управлению информационными ресурсами. Методы управления инновациями в данной области имеют огромное значение, поскольку позволяют эффективно защищать данные и обеспечивать безопасность информационных систем. Рассмотрим основные из них:

1. Применение технологий и систем безопасности, таких как антивирусное и антишпионское программное обеспечение, брандмауэры, шифрование данных и прочие. Наиболее известной технологией является криптография. Криптография – это технология преобразования данных, с помощью которой они становятся зашифрованными с помощью специальных ключей или методов. Криптографические методы используют, например, государственные учреждения для создания цифровых подписей, банки — для денежных переводов, пользователи — когда заходят в интернет с подключенным VPN [1].

Технология Блокчейн основана на принципе децентрализованного хранения данных. Данные разделяются на блоки (от англ. block), каждый из блоков связан с предыдущим, тем самым выстраивая цепочку (от англ. chain). Изменения данных в предыдущих блоках является ресурсоёмким процессом и в большинстве случаев невозможным. Все, что попадает в сеть блокчейна, остается в неизменном состоянии навсегда. Этот способ используют, например, в здравоохранении — организации хранят в блокчейне медицинские карты пациентов.

Брандмауэр — технология, которая предоставляет защитный экран между устройством и внешними сетями. С помощью брандмауэра можно, например, распределить трафик между устройствами и ограничить доступ к определённым ресурсам. Брандмауэры устанавливают, например, в школах, чтобы оградить детей от запрещённого или опасного контента. Или в организациях, чтобы заблокировать спам, отправляемый потенциальными злоумышленниками на электронные почты сотрудников. Очевидно, что применение современных технологий как метода управления инновациями в обеспечении безопасности в экономических информационных системах трудно переоценить. Таким образом, применение современных технологий, предприятия и организации могут защитить конфиденциальные данные, обеспечить непрерывность бизнеса, соблюдать нормативные акты и поддерживать свою деловую репутацию, личную безопасность и доверие своих клиентов.

2. Проведение аудита системы безопасности для выявления уязвимостей и угроз. Аудит безопасности играет важную роль в обеспечении защиты информации и выявлении уязвимостей в системах. Проведение анализа и тестирования компонентов безопасности позволяет определить реальные уровни защиты и выявить области, требующие улучшений. Полученные данные после аудита помогают разработать и внедрить необходимые меры по укреплению системы безопасности, что в свою очередь снижает вероятность успешных атак или инцидентов безопасности.

Проведение аудита позволяет также выявить потенциальные угрозы, определить векторы атаки, выявить технические уязвимости и слабые места в сети. Это позволяет специалистам по безопасности разработать стратегию усиления защиты на выявленных уровнях. Таким образом, аудит безопасности является неотъемлемой частью комплексной стратегии защиты IT-инфраструктуры, обеспечивая высокий уровень безопасности и защиту данных организации.

3. Обучение и повышение квалификации сотрудников по вопросам информационной безопасности.

В связи с тем, что угрозы кибербезопасности постоянно эволюционируют, компании должны быть готовы к защите своих данных и информационных ресурсов. Одним из ключевых моментов в обеспечении безопасности является обучение и повышение квалификации сотрудников по вопросам информационной безопасности. Человеческий

фактор часто является слабым звеном в цепи безопасности, поэтому обучение персонала помогает уменьшить риски, связанные с недостаточным осведомленностью сотрудников.

Преимуществами обучения сотрудников по информационной безопасности являются:

– повышение осведомленности: обученные сотрудники лучше понимают угрозы информационной безопасности и знают, как правильно реагировать на них.

– снижение рисков: обученные сотрудники могут помочь предотвратить утечки данных, кибератаки и другие угрозы, что способствует снижению рисков для компании.

– соответствие законодательству: обучение сотрудников по вопросам информационной безопасности помогает компании соблюдать требования законодательства в области защиты данных.

– улучшение репутации: компании, которые серьезно относятся к вопросам информационной безопасности и обучают свой персонал, создают положительное впечатление на клиентов и партнеров [3].

Существует множество методов обучения сотрудников по вопросам информационной безопасности. Самым удобными способом обучения являются онлайн-курсы и вебинары, которые позволяет сотрудникам получить знания в удобное время. В последнее время достаточно эффективным показала себя симуляция кибератак. При проведении учебных симуляций сотрудники могут попрактиковаться в реагировании на реальные угрозы. В любом случае обучение по вопросам информационной безопасности должно быть постоянным процессом, так как угрозы постоянно меняются.

Бесспорно, обучение и повышение квалификации сотрудников по вопросам информационной безопасности является важным элементом в обеспечении безопасности компании. Инвестирование в обучение персонала помогает снизить риски киберугроз и защитить бизнес от потенциальных угроз. В конечном итоге, обученные сотрудники становятся ценным активом для компании в борьбе за информационную безопасность.

4. Разработка и внедрение политики безопасности информационной системы.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности и Доктрина Информационной безопасности. Политика безопасности (далее ПБ) строится на основе анализа рисков, которые признаются реальными для информационной системы организации. После того, как проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Результативный уровень информационной безопасности в современной организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективной политики безопасности. Эффективные ПБ определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Что бы ПБ оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах ИБ и обучать их выполнению правил, предписываемых ПБ. Регулярный пересмотр и корректировка правил ПБ необходимы для поддержания ее в актуальном состоянии [4].

5. Использование международных стандартов и регуляций в области информационной безопасности, таких как ISO 27001.

ISO 27001 — это стандарт «Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования и определения». Цель стандарта ISO 27001 — определение и установка требований для создания, внедрения, поддержания функционирования и непрерывного улучшения системы менеджмента информационной безопасности. Стандарт ISO 27001 включает требования для оценки и обработки рисков информационной безопасности, адаптированных к потребностям организации. Стандарт ISO/IEC 27001 является международным и устанавливает требования к системам управления информационной безопасностью (СИУБ). С его

помощью организации защищают свои информационные активы путем систематического подхода к управлению конфиденциальной информацией и обеспечению безопасности информации, включая финансовые данные, интеллектуальную собственность, данные сотрудников и информацию, передаваемую третьим лицам. Применение ISO/IEC 27001 – обязательное требованием в некоторых регулируемых отраслях. Кроме того, сертификация по данному стандарту помогает организациям управлять рисками и повышать эффективность операций. Стандарт ISO/IEC 27001 признан на международном уровне, что расширяет ваши возможности для ведения глобального бизнеса и участия в международных тендерах.

6. Тестирование на проникновение, или пентест – это санкционированная смоделированная кибератака на компьютерную систему компаний и организаций, выполняемая для оценки безопасности системы. Специалисты по тестированию на проникновение используют те же инструменты, методы и процессы, что и злоумышленники, так называемые субъекты киберугроз, чтобы найти и продемонстрировать влияние слабых мест в системе на бизнес.

Тестирование на проникновение осуществляется в форме имитации различных атак, которые могут угрожать бизнесу. Целью тестирование является проверка надежности системы и ее возможность противостоять атакам с аутентифицированных и не аутентифицированных позиций. При правильном охвате пентест может проникнуть в любой аспект системы [2].

С операционной точки зрения тестирование на проникновение помогает сформировать стратегию информационной безопасности за счет быстрого и точного выявления уязвимостей. Как следствие - устранение выявленных рисков и осуществление корректирующих действий, а также расширение знаний в области информационной безопасности.

Тестирование на проникновение предоставляет подробную информацию о реальных угрозах безопасности, которые могут быть использованы в преступных целях. Это поможет организации быстро и точно определить реальные и потенциальные уязвимости. Этот метод также может помочь организации количественно оценить последствия и вероятность уязвимостей, что позволит организации расставить приоритеты и принять корректирующие меры для сообщений об известных уязвимостях.

7. Интеграция новых технологий и инноваций в области безопасности для улучшения защиты информационных систем.

Новые технологии могут помочь усилить защиту от угроз, а также обнаруживать и предотвращать атаки на ранних стадиях [3].

Одной из ключевых технологий в области безопасности является искусственный интеллект (ИИ). С его помощью можно создать системы мониторинга, которые способны анализировать большие объемы данных и выявлять аномалии в поведении пользователей или в сети. Такие системы могут помочь предотвратить утечки данных или атаки на систему до их нанесения ущерба.

Также важно интегрировать новейшие методы шифрования данных, механизмы аутентификации и авторизации, а также системы мониторинга и обнаружения угроз. Такие решения позволят усилить защиту информационных систем и предотвратить утечки или атаки.

В целом, интеграция новых технологий и инноваций в области безопасности играет важную роль в повышении уровня защиты информационных систем. Компании и организации должны постоянно следить за новейшими разработками и внедрять их для обеспечения надежной защиты от угроз.

Основные сложности, с которыми сталкиваются компании при внедрении инноваций в области безопасности.

Внедрение инноваций в области информационной безопасности может стать серьезным испытанием для компаний и госучреждений. Несмотря на важность этих шагов,

компании сталкиваются с рядом трудностей. Здесь мы рассмотрим основные сложности, с которыми встречаются организации при внедрении инноваций в области безопасности.

Одной из первых и наиболее распространенных проблем является сопротивление изменениям как со стороны руководства, так и со стороны сотрудников. Люди по своей природе склонны избегать перемен, особенно если они связаны с внедрением новых технологий. Существует риск, что работники не будут готовы адаптироваться к новым процессам и инструментам, что может привести к снижению эффективности и безопасности. Важно правильно организовать процесс изменений и обеспечить обучение персонала, чтобы минимизировать это сопротивление.

Внедрение современных технологий безопасности часто требует значительных финансовых вложений. Это может включать не только закупку оборудования и программного обеспечения, но и обучение сотрудников, изменения в инфраструктуре и другие сопутствующие расходы. Многие компании останавливаются на полурешениях, что подрывает общую эффективность защиты. Компании важно проводить тщательный анализ затрат и выгод, чтобы четко понимать, оправданы ли инвестиции.

При внедрении новых технологий важно учитывать существующие системы безопасности. Интеграция новых решений с уже установленными может представлять собой сложную задачу, требующую времени и усилий. Неправильная интеграция может привести к уязвимостям и снижению общего уровня безопасности. Поэтому важно заранее планировать процесс внедрения, привлекая специалистов, которые помогут в этой задаче.

С введением новых технологий часто возникают опасения по поводу защиты личных данных. Инновационные решения могут направляться на сбор и анализ больших объемов информации, что может вызвать негативную реакцию со стороны клиентов и общественности. Компании должны быть готовы к обеспечению прозрачности своих действий, а также соблюдению всех норм и правил, касающихся конфиденциальности данных.

Мир технологий и безопасности не стоит на месте. Киберугрозы и методы их реализации постоянно эволюционируют, и компаниям нужно оставаться на шаг впереди. Это требует постоянной адаптации внедряемых решений и пересмотра стратегий безопасности. Некоторым организациям сложно быть в курсе последних тенденций и угроз, что делает их уязвимыми.

Для успешной реализации инноваций в области безопасности необходимы квалифицированные специалисты. Однако на рынке труда часто наблюдается дефицит таких кадров. Компании могут столкнуться с трудностями при подборе специалистов, что замедляет процесс внедрения новых технологий. Важно не только нанимать новых сотрудников, но и инвестировать в обучение и развитие существующих кадров.

Таким образом, внедрение инноваций в области безопасности — сложный, но необходимый процесс. Осознание основных трудностей позволяет компаниям заранее подготовиться к преодолению этих преград. Работая над устранением этих проблем, организации могут значительно повысить уровень своей безопасности и защитить как свои активы, так и данные клиентов. Успешная реализация инновационных решений станет залогом не только повышения эффективности, но и укрепления доверия со стороны клиентов и партнеров.

Рекомендации по дальнейшему развитию и улучшению методологий управления инновациями в обеспечении безопасности в экономических информационных системах

Эффективное управление инновациями в данной области предполагает интеграцию новых методов и подходов, что требует адаптации и постоянного совершенствования существующих методологий. Рассмотрим рекомендации для дальнейшего развития и улучшения методологий управления инновациями в обеспечении безопасности в ЭИС.

1. Внедрение гибких методологий управления проектами

Современные условия требуют от организаций быстрой реакции на изменения и адаптации к новым угрозам. Гибкие методологии управления проектами, такие как Agile или Scrum, позволяют командам оперативно реагировать на изменения, вносить корректировки в проекты на различных этапах, а также эффективно управлять ресурсами. Это особенно актуально для проектов в сфере безопасности, где высока степень неопределенности и динамичности.

2. Создание междисциплинарных команд

Инновации в области безопасности требуют участия специалистов из различных областей: IT, юриспруденции, управления рисками и др. Формирование междисциплинарных команд поможет объединить знания и опыт, что максимально повысит эффективность разработки и внедрения новых решений. Важно обеспечить обмен информацией и идеями между всеми участниками процесса, что способствует кросс-функциональному подходу к решению задач.

3. Повышение осведомленности и образования персонала

Человеческий фактор остается одной из главных уязвимостей для системы безопасности. Обучение и повышение осведомленности сотрудников о современных угрозах и методах защиты должны стать постоянной практикой. Регулярные тренинги, семинары и курсы по кибербезопасности помогут сотрудникам лучше осознавать риски и применять соответствующие методы защиты. Инвестирование в образование персонала не только минимизирует возможные угрозы, но и способствует развитию инновационного мышления внутри организации.

4. Использование передовых технологий.

С учетом текущих трендов развития технологий, таких как искусственный интеллект, машинное обучение и блокчейн, компании должны активно исследовать возможности их применения для повышения безопасности ЭИС. Эти технологии имеют потенциал не только для автоматизации процессов, но и для улучшения анализа рисков, мониторинга угроз и выявления аномалий. Внедрение этих инноваций может значительно повысить уровень защиты и уменьшить временные затраты на реагирование.

5. Устойчивое управление рисками.

Совершенствование методологий управления рисками должно стать ключевым аспектом управления инновациями в области безопасности. Необходимо разработать системы регулярного анализа и оценки рисков, внедряя практики мониторинга и аудита. Это позволит не только своевременно выявлять потенциальные угрозы, но и снижать вероятность их реализации. Актуальные системы управления рисками позволят оперативно адаптировать меры безопасности к изменяющимся условиям.

6. Разработка стандартов и регламентов

Установление четких стандартов и регламентов по обеспечению безопасности в ЭИС поможет унифицировать подходы и улучшить взаимодействие между различными подразделениями. Это обеспечит более высокую степень координации действий, повысит уровень ответственности и научит работников правильно применять новые инструменты и технологии. Акцент на стандартизацию также позволит повысить доверие со стороны клиентов и партнеров [1].

Управление инновациями в обеспечении безопасности в экономических информационных системах требует комплексного подхода и постоянного совершенствования. Внедрение гибких методологий, создание междисциплинарных команд, повышение уровня осведомленности и использование передовых технологий станут залогом успеха в борьбе с растущими угрозами. Следуя указанным рекомендациям, организации смогут не только повысить уровень безопасности своих систем, но и значительно укрепить позиции на рынке, гарантируя клиентам защиту их данных и информации.

Список источников

1. Авдеева И.Л., Ананченкова П.И., Белолипецкая А.Е., Боброва Е.А., и др. Интеграция кадровой политики в систему управления национальными проектами. Монография. – Орел: Среднерусский институт управления - филиал РАНХиГС, 2020.

2. Бабуркина А.С., Широкова С.В., Ильяшенко О.Ю. Разработка процедуры проведения аудита безопасности информационной системы для ООО «Клиника современной косметологии» // Фундаментальные и прикладные исследования в области управления, экономики и торговли. Сборник трудов научной и учебно-практической конференции: в 3 частях. 2017. С. 15–22.

3. Зайченко И.М., Горшечникова П.Д., Лёвина А.И., Дубгорн А.С. Цифровая трансформация бизнеса: подходы и определение // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2020. № 2. С. 205–212.

4. Зайченко И.М., Смирнова А.М. Анализ инновационных стратегий в условиях цифровой трансформации бизнеса // Научный вестник Южного института менеджмента. 2019. № 2. С. 12–17.

5. Цифровая трансформация бизнеса на основе технологии искусственного интеллекта//Актуальные вопросы современной экономики. 2021.- №10. С.199-202

Информация об авторе

Востряков Владимир Сергеевич, аспирант Московской международной академии, г. Москва, Россия

Information about the author

Vostryakov Vladimir Sergeevich, PhD student at the Moscow International Academy, Moscow, Russia