БЕЗОПАСНАЯ РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: АНАЛИЗ ВЫГОД И ПРЕПЯТСТВИЙ НА ПУТИ К УСПЕШНОЙ ИНТЕГРАЦИИ

Левчук А. Т. *
магистр
alevchuk-19@edu.ranepa.ru

Научный руководитель:
Нестеренко Ю. Н. *
д.э.н., профессор
julia-nesterenko@mail.ru

* Российская Академия Народного Хозяйства и Государственной Службы при Президенте Российской Федерации,
г. Москва, Россия

Аннотация:
В научной статье рассматривается безопасная разработка программного обеспечения (БРПО), ее ключевые компоненты и роль в обеспечении безопасности на всех этапах жизненного цикла разработки ПО (SSDLC). Автор приводит определение БРПО и описывает основные организационные и технические меры, включая формирование нормативной базы, проведение тренингов для сотрудников, использование инструментов для автоматизированного анализа кода и проведение контролируемых атак на систему. В статье анализируются преимущества внедрения БРПО, а также рассматриваются барьеры на пути к ее успешной интеграции. В заключении предлагаются рекомендации для компаний, направленные на преодоление этих препятствий и обеспечение эффективного внедрения безопасной разработки программного обеспечения.

Ключевые слова:
безопасная разработка, преимущества БРПО, барьеры интеграции, жизненный цикл ПО, организационные меры, технические меры, рекомендации для компаний.

УДК 334(075.8)
DOI: 10.24411/2658-6932-2024-02-21-29

Для цитирования: Левчук А. Т. Безопасная разработка программного обеспечения: анализ выгод и препятствий на пути к успешной интеграции / А. Т. Левчук, Ю. Н. Нестеренко // Контентус. – 2024. – №2. – С. 21 – 29.

Безопасная разработка программного обеспечения (далее сокращенно – БРПО) представляет собой совокупность процессов и практик, интегрируемых в жизненный цикл разработки программного обеспечения (SSDLC) с целью обеспечения безопасности на всех его этапах. БРПО направлена на предотвращение, выявление и устранение уязвимостей и угроз, которые могут возникнуть в ходе создания и эксплуатации программных продуктов.

Жизненный цикл разработки программного обеспечения (SSDLC) традиционно включает следующие этапы:

1. Определение целей проекта, сбор и анализ требований к ПО.
2. Разработка архитектуры системы и детального дизайна компонентов.
3. Написание исходного кода в соответствии с проектной документацией.
4. Проверка корректности и безопасности разработанного ПО.
5. Развертывание ПО в рабочей среде и его эксплуатация.
6. Обеспечение работоспособности и обновление ПО.

Интеграция мер безопасности на каждом этапе SSDLC позволяет минимизировать риски, связанные с эксплуатацией программных систем, и обеспечивает более высокий уровень защиты данных и инфраструктуры.

Для эффективного внедрения БРПО используются как организационные, так и технические меры.

Организационные меры включают в себя [4]:

1. Формирование нормативной базы, регламентирующей процессы безопасной разработки.
2. Проведение тренингов и семинаров для разработчиков и сотрудников ИБ, направленных на повышение их осведомленности и навыков в области безопасности.
3. Включение специалистов по безопасности на всех этапах разработки, что способствует раннему выявлению и устранению уязвимостей.

Технические меры включают:

1. Использование инструментов для автоматизированного анализа исходного кода с целью выявления потенциальных уязвимостей.
2. Проведение контролируемых атак на систему для выявления и устранения слабых мест.
3. Внедрение инструментов и методологий, таких как Secure Coding Guidelines, SAST (Static Application Security Testing) и DAST (Dynamic Application Security Testing).

Примеры стандартов и регламентов, применяемых в рамках БРПО, включают национальные стандарты, такие как ГОСТ Р ИСО/МЭК 27034-2014 (Информационные технологии – Безопасность процессов разработки программного обеспечения) [2], ГОСТ Р ИСО/МЭК 15408-2012 (Критерии оценки безопасности информационных технологий) [1] и ГОСТ Р 56939-2016 (Разработка безопасного программного обеспечения – Общие требования) [3].

Внедрение БРПО способствует значительному сокращению затрат на разработку и эксплуатацию программных продуктов. Во-первых, стандартизация процессов и инструментов разработки позволяет снизить требования к квалификации разработчиков и упростить адаптацию новых сотрудников. Это, в свою очередь, ведет к снижению расходов на обучение и привлечение специалистов. Кроме того, унифицированные процессы обеспечивают более предсказуемое планирование и контроль над проектами, что снижает вероятность перерасхода бюджета.

Вторым важным аспектом является сокращение совокупной стоимости владения (ТСО) автоматизированными системами и информационными системами (АС/ИС). За счет повышения стабильности релизов и уменьшения количества исправлений и доработок после ввода в эксплуатацию, компании могут значительно снизить расходы на сопровождение и поддержку ПО. Вдобавок, встроенные механизмы безопасности уменьшают необходимость в дополнительных инвестициях в защитные решения, что также снижает общие затраты.

Одним из ключевых преимуществ внедрения БРПО является повышение стабильности релизов программных продуктов. Это достигается за счет улучшения транспарентности (прозрачности) процесса разработки и выявления уязвимостей на самых ранних стадиях. Выявление и устранение проблем на этапе разработки значительно дешевле и эффективнее, чем в последующих стадиях жизненного цикла ПО.

Повышение управляемости процесса внедрения автоматизированных информационных систем (АИС) также является важным техническим преимуществом. Благодаря четко выстроенным процессам и регулярным проверкам на соответствие требованиям безопасности, компании могут быстрее и с меньшими рисками внедрять новые решения. Это ведет к сокращению сроков внедрения и улучшению контроля над проектами, что положительно сказывается на общей операционной эффективности.

Внедрение БРПО помогает компаниям обеспечить непрерывность бизнеса за счет снижения рисков информационной безопасности (ИБ), связанных с эксплуатацией автоматизированных систем. Надежные и проверенные на безопасность решения снижают вероятность инцидентов, которые могут привести к остановке бизнеса или утрате данных.

Минимизация комплаенс-рисков и соответствие требованиям регуляторов являются еще одним значимым преимуществом. В современных условиях, когда требования к информационной безопасности ужесточаются, компании, внедряющие БРПО, могут быть уверены в том, что их процессы соответствуют международным и отраслевым стандартам. Это не только уменьшает риски получения штрафов и санкций, но и улучшает репутацию компании на рынке.

Несмотря на явные преимущества безопасной разработки программного обеспечения, компании сталкиваются с множеством значительных трудностей при интеграции этих практик. Одной из главных организационных преград является обоснование необходимости внедрения БРПО. Менеджеры и руководители проектов часто сталкиваются с проблемой аргументации инвестиций в безопасность на этапе разработки, поскольку выгоды таких вложений могут быть неочевидны и проявляются в долгосрочной перспективе.

Важным препятствием является также внутреннее сопротивление изменениям среди сотрудников. Пересмотр устоявшихся рабочих практик и внедрение новых процессов часто вызывает естественное сопротивление со стороны разработчиков и других участников процесса, что может быть связано с опасениями относительно увеличения объема работы, необходимостью освоения новых технологий или страхом перед неопределенностью.

Кроме того, проблема состоит в нехватке специалистов с глубокими знаниями в области информационной безопасности. Привлечение и удержание таких экспертов может быть сложной задачей, особенно при ограниченном бюджете. Недостаток квалифицированных кадров затрудняет реализацию всех необходимых мер по БРПО.

Разработчики и менеджеры проектов могут опасаться, что новые меры безопасности нарушат текущие рабочие процессы, приведут к задержкам в разработке и снизят продуктивность. Для минимизации негативных последствий и обеспечения плавного перехода к новым практикам необходима тщательная подготовка и планирование.

Консалтинговые услуги играют ключевую роль в успешном внедрении безопасной разработки программного обеспечения. Привлечение внешних экспертов позволяет компании воспользоваться их опытом и знаниями для создания эффективных и адаптированных к специфике организации процессов. Консультанты помогают проводить независимую оценку текущих процессов разработки ПО, выявляя слабые места и предлагая рекомендации по их оптимизации.

Одним из основных преимуществ консалтинговых услуг является гибкий проектный подход, который гарантирует достижение

результатов в установленные сроки и с учетом ресурсных ограничений. Консультанты разрабатывают технические задания по информационной безопасности для автоматизированных информационных систем, ориентируясь на производственные процессы, актуальную модель угроз и требования регуляторов.

Внедрение БРПО представляет собой многоэтапный процесс, включающий следующие ключевые этапы:

1. Подготовка ТЭО. На данном этапе проводится определение целей и задач проекта, а также разработка технико-экономического обоснования (ТЭО), что помогает убедить руководство в необходимости внедрения БРПО.

2. Аудит текущих процессов. Проведение детального обследования текущих бизнес-процессов разработки позволяет выявить существующие недостатки и определить целевое состояние процесса БРПО в соответствии с требованиями регуляторов.

3. Разработка плана перехода и дорожной карты. На этом этапе формируется план перехода к новым процессам, включающий детализированные рекомендации по внедрению БРПО. Разработка дорожной карты помогает четко определить последовательность действий и сроки реализации проекта.

4. Внедрение процессов и контроль. Реализация организационных и технических мер по внедрению БРПО осуществляется в соответствии с разработанным планом. Контрольные мероприятия проводятся для проверки соответствия достигнутого состояния установленным требованиям и целям проекта.

Для успешной интеграции БРПО автор рекомендует использовать следующие меры:

1. Регулярное проведение тренингов и семинаров по безопасности позволит разработчикам и другим сотрудникам лучше понимать важность безопасности и эффективно применять новые знания на практике.

2. Включение специалистов по безопасности в команды разработки поможет раннему выявлению уязвимостей и обеспечит более высокий уровень защиты программного обеспечения.

3. Адаптация методологий и инструментов под конкретные условия и потребности компании позволит более эффективно интегрировать БРПО в существующие процессы.

4. Постоянный мониторинг и оценка процессов разработки и безопасности помогут своевременно выявлять и устранять новые угрозы и уязвимости.

Таким образом, комплексный подход к внедрению БРПО, основанный на лучших практиках и опыте внешних консультантов, позволит компании не только обеспечить высокую степень безопасности своих

программных продуктов, но и повысить общую эффективность и конкурентоспособность на рынке.

Список использованных источников

1. ГОСТ Р ИСО/МЭК 15408-2012 «Информационная технология. МЕТОЖЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ» [Электронный ресурс]. Режим доступа: https://files.stroyinf.ru/Data2/1/4293781/4293781374.pdf
2. ГОСТ Р ИСО/МЭК 27034-2014 «Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Безопасность приложений» [Электронный ресурс]. Режим доступа: https://files.stroyinf.ru/Data2/1/4293768/4293768990.pdf
3. ГОСТ Р 56939-2016 «Защита информации. РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Общие требования» [Электронный ресурс]. Режим доступа: https://files.stroyinf.ru/Data2/1/4293754/4293754625.pdf
4. **Черемисин Д.Г., Мкртчян В.Р.** Безопасная разработка программного обеспечения / Д.Г. Черемисин, В.Р. Мкртчян // Международный научный журнал «Символ науки», №6-2, 2023 г. – 27-28 стр.

SAFE SOFTWARE DEVELOPMENT: ANALYSIS OF BENEFITS AND BARRIERS TO SUCCESSFUL INTEGRATION

Levchuk A. T. **
master's student
alevchuk-19@edu.ranepa.ru

Research supervisor:
Nesterenko J. N. **
Doctor of Economics, professor
julia-nesterenko@mail.ru

**Russian Presidential Academy of National Economy and Public Administration,
Moscow, Russia

Abstract:
The scientific article examines secure software development (SSD), its key components, and its role in ensuring security at all stages of the software development lifecycle (SDLC). The author defines SSD and describes the main organizational and technical measures, including the formation of a regulatory framework, conducting employee training, using tools for automated code analysis, and performing controlled attacks on the system. The article analyzes the advantages of implementing SSD, as well as the barriers to its successful integration. The conclusion offers recommendations for companies aimed at overcoming these obstacles and ensuring the effective implementation of secure software development.

Keywords:
secure development, advantages of SSD, integration barriers, software lifecycle, organizational measures, technical measures, recommendations for companies.