БАНК РАЗВИТИЯ

ПРАКТИЧЕСКИЕ АСПЕКТЫ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

САВИЧ Валерий Вениаминович
заместитель начальника управления - начальник отдела информационной безопасности Управления информационной безопасности и охраны

СТАДИИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

БАНК РАЗВИТИЯ

1. 

ОБОСНОВАНИЕ ПРОВЕДЕНИЯ ЗАКУПКИ И ВНЕДРЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ. УТВЕРЖДЕНИЕ СТРАТЕГИИ РАЗВИТИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАНКА.

2. 

ИЗУЧЕНИЕ РЫНКА, ПРОВЕДЕНИЕ ПИЛОТНЫХ ПРОЕКТОВ ПЛАНИРУЕМЫХ К ВНЕДРЕНИЮ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

3. 

ФОРМИРОВАНИЕ И УТВЕРЖДЕНИЕ ТРЕБОВАНИЙ ДЛЯ ПЛАНИРУЕМОЙ К ВНЕДРЕНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

- функциональные требования
- технические требования
- требования по информационной безопасности
- требования к документации, внедрению, сервисному и техническому обслуживанию

4. 

ПРОВЕДЕНИЕ КОНКУРЕНТНЫХ ПРОЦЕДУР ЗАКУПОК

5. 

ЭТАПЫ ЖИЗНЕННОГО ЦИКЛА (ТРЕБОВАНИЯ ГЛАВЫ 5 СФУТ 9.01-2024)

- разработка технических заданий
- проектирование
- создание и тестирование
- приемка, включая оценку соответствия
- ввод в эксплуатацию и эксплуатация
- сопровождение и модернизация
- вывод из эксплуатации

КЛЮЧЕВЫЕ ФАКТОРЫ УСПЕШНОЙ РЕАЛИЗАЦИИ ПРОЕКТОВ

БАНК РАЗВИТИЯ

ПОДДЕРЖКА РУКОВОДСТВА

Целесообразно разработать и утвердить долгосрочную Стратегии развития системы обеспечения безопасности Банка.

ВЫДЕЛЕНИЕ РЕСУРСОВ

Для реализации проекта необходимы финансовые, кадровые и технические ресурсы.

КВАЛИФИЦИРОВАННЫЙ ПЕРСОНАЛ

Лучшая реализация проекта достигается при привлечении персонала, имеющего опыт эксплуатации и внедрения соответствующих средств защиты информации.

СОТРУДНИЧЕСТВО

Должно быть обеспечено конструктивное взаимодействие между различными подразделениями, задействованными во внедрении проекта (ИТ, безопасность, бизнес подразделения).

ИТЕРАТИВНЫЙ ПОДХОД

Используйте итеративный подход по созданию системы защиты информации, позволяющий гибко адаптироваться к изменениям и вносить необходимые корректировки.

ВАЖНО ПОМНИТЬ: Создание и поддержание СЗИ – это непрерывный процесс. Необходимо постоянно следить за изменениями в ландшафте угроз, развитием технологий и совершенствовать свою систему защиты.

Кроме того, важно учитывать специфику организации, ее размер, используемые технологии и другие факторы.

ОБОСНОВАНИЕ ВНЕДРЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

БАНК РАЗВИТИЯ

ОБОСНОВАНИЕ МОЖЕТ ВКЛЮЧАТЬ СЛЕДУЮЩИЕ ПУНКТЫ

АКТУАЛЬНОСТЬ

Почему данная закупка необходима именно сейчас. Необходимо сделать ссылки на выявленные уязвимости, изменившиеся требования регуляторов, новые угрозы и т.д.

СООТВЕТСТВИЕ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

Как правило внедрение будет поддержано если оно осуществляется в соответствии с требованиями законодательства, приказов ОАЦ, утвержденной Стратегии развития систем обеспечения безопасности, отраслевых стандартов.

ЦЕЛИ И ЗАДАЧИ

Какие конкретные цели и задачи будут достигнуты в результате внедрения.

ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

Необходимо проработать основные функциональные возможности, которые должны быть реализованы в рамках внедрения. Это поможет обосновать выбор конкретного решения/продукта.

ОЖИДАЕМЫЙ ЭФФЕКТ

Укажите, какие положительные изменения произойдут в результате внедрения.

ВЛИЯНИЕ НА СУЩЕСТВУЮЩУЮ ИНФРАСТРУКТУРУ

Проведите оценку совместимости планируемой закупки с существующими системами. Возможно потребуется разработка отдельной методики оценки влияния на инфраструктуру.

ПОСЛЕДСТВИЯ ОТСУТСТВИЯ ЗАКУПКИ

Укажите, какие негативные последствия могут возникнуть, если закупка не будет произведена (увеличение рисков, нарушение законодательства, снижение эффективности работы). При наличии дополнительных рисков необходимо проработать мероприятия по их минимизации.

ОСНОВНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ ДЛЯ ОБОСНОВАНИЯ ЗАКУПКИ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

БАНК РАЗВИТИЯ

ЗАКОНЫ РЕСПУБЛИКИ БЕЛАРУСЬ

- «Об информации, информатизации и защите информации» (от 10.11.2008 № 455-З)
- «О защите персональных данных» (от 7.05.2021 № 99-З)
- «Об электронном документе и электронной цифровой подписи» (от 28.12.2009 № 113-З)

УКАЗЫ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ

- «О некоторых мерах по совершенствованию защиты информации» (от 16.04.2013 № 196)
- «О кибербезопасности» (от 14.02.2023 № 40)
- «О совершенствовании государственного регулирования в области защиты информации» (от 9.12.2019 № 449)

ПОСТАНОВЛЕНИЯ СОВЕТА МИНИСТРОВ РЕСПУБЛИКИ БЕЛАРУСЬ:

- «Об утверждении технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/BY)» (от 15.05.2013 № 375)
- «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. №40» (от 23.02.2024 № 120)

ПРИКАЗЫ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ:

- «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 (от 20.02.2020 № 66) (далее – Приказ ОАЦ № 66)
- «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» (от 25.07.2023 № 130)

ПОСТАНОВЛЕНИЯ ПРАВЛЕНИЯ НАЦИОНАЛЬНОГО БАНКА РЕСПУБЛИКИ БЕЛАРУСЬ

- «Об утверждении Инструкции о требованиях по защите информации и обеспечению кибербезопасности при оказании платежных услуг» (от 6.10.2022 № 377)
- «О предоставлении информации об инцидентах и нарушениях безопасности в сфере защиты информации“ (от 15.12.2023 № 454)

ОСНОВНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ ДЛЯ ОБОСНОВАНИЯ ЗАКУПКИ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

БАНК РАЗВИТИЯ

СТАНДАРТЫ ФИНАНСОВЫХ УСЛУГ И ТЕХНОЛОГИЙ:

- СФУТ 9.01-2024 «Банковская деятельность. Обеспечение информационной безопасности. Общие положения и терминология» (постановление Правления Национального банка Республики Беларусь от 20.06.2024 № 185)

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ПРАВИЛА

- ТТП ИБ 2.1 – 2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Требования к системам менеджмента информационной безопасности»
- ТТП ИБ 4.1 – 2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Менеджмент рисков информационной безопасности»
- ТТП ИБ 9.1 – 2022 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Ресурсное обеспечение информационной безопасности»

СТАНДАРТЫ РЕСПУБЛИКИ БЕЛАРУСЬ 34 СЕРИИ:

- СТБ 30.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014, СТБ 34.101.8-2006, СТБ 34.101.14-2017, СТБ 34.101.14-2017, СТБ 34.101.74-2017, СТБ 34.101.73-2017, СТБ 34.101.75-2017

СТАНДАРТ БЕЗОПАСНОСТИ ДАННЫХ ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ (PCI DSS)

СТРАТЕГИЯ РАЗВИТИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАНКА

ИЗУЧЕНИЕ РЫНКА, ПРОВЕДЕНИЕ ПИЛОТНЫХ ПРОЕКТОВ

БАНК РАЗВИТИЯ

ИЗУЧЕНИЕ РЫНКА

Перед формированием требований изучите рынок существующих продуктов и решений в области ИБ

АНАЛИЗ ДОКУМЕНТАЦИИ

Изучите документацию на продукты, обращая внимание на их функциональные возможности, технические характеристики и соответствие требованиям безопасности

СРАВНЕНИЕ ПРОДУКТОВ

Сравните различные продукты между собой, чтобы выбрать наиболее подходящий для ваших нужд

УЧЕТ СТОИМОСТИ ВЛАДЕНИЯ

Учитывайте не только стоимость приобретения продукта, но и стоимость его внедрения, настройки и поддержки

ПРОВЕДЕНИЕ ПИЛОТНЫХ ПРОЕКТОВ

ЦЕЛИ:

- Оценить, насколько хорошо выбранные продукты соответствуют требованиям и как они работают в реальных условиях.
- Оценить влияние продуктов на инфраструктуру
- Определить количество лицензий, необходимых для закупки
- Уточнить и проработать требования к внедряемой системе
- Получить первичный опыт эксплуатации системы, выявить ее недостатки и положительные характеристики
- Использовать имеющиеся настройки системы и ноу-хау (правила, инструментальные панели, листы) для последующего внедрения в аналогичную систему

ВЫБОР УЧАСТНИКОВ

Привлеките к пилотированию представителей различных подразделений

РАЗРАБОТКА СЦЕНАРИЕВ ТЕСТИРОВАНИЯ

Разработайте сценарии тестирования, которые охватывают все основные функции системы

СБОР ОБРАТНОЙ СВЯЗИ

Соберите обратную связь от участников пилотирования

АНАЛИЗ РЕЗУЛЬТАТОВ

Проанализируйте результаты пилотирования и примите решение о внедрении системы

ОБЩАЯ СТРУКТУРА ТРЕБОВАНИЙ

БАНК РАЗВИТИЯ

1. ВВЕДЕНИЕ

Цель документа, область применения, термины и сокращения.

2. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

Разделенные по функциям системы, с детализацией каждой функции.

3. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

Производительность, надежность, совместимость, интеграция.

4. ТРЕБОВАНИЯ ПО ИБ

СТБ 34 серии, политики безопасности, уровни доступа, протоколирование, антивирусная защита и т.д.

5. ТРЕБОВАНИЯ ПО ВНЕДРЕНИЮ

6. ПРИЛОЖЕНИЯ

Подробное описание проводимых настроек по конкретной системе (при необходимости).

ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ ДЛЯ СРЗИ

ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ ДЛЯ СРЗИ ВКЛЮЧАЮТ СЛЕДУЮЩИЕ РАЗДЕЛЫ

- общие требования к системе
- требования к подсистемам управления активами, инцидентами ИБ (если применимо)
- требования к подсистеме сбора и фильтрации (если применимо)
- требования к подсистеме регистрации и аудита
- требования к подсистеме визуализации и аналитики
- требования к интерфейсу
- требования к архитектуре и развертыванию
- требования к лицензированию

ВЕСОВЫЕ КОЭФФИЦИЕНТЫ И ОБЯЗАТЕЛЬНОСТЬ ТРЕБОВАНИЙ

Обязательные требования - требования которые должны выполняться системой в обязательном порядке и должны быть выполнены на этапе внедрения.

ВЕСОВЫЕ КОЭФФИЦИЕНТЫ (для необязательных требований):

10	необязательные требования, соответствие которым позволяет с максимальным объёмом и качеством, а также необходимой степенью автоматизации осуществлять деятельность по обеспечению ИБ в рамках функционирования системы (для функциональных требований), либо является необходимым условием для функционирования подсистем ИБ прикладного ПО (для требований по ИБ)
5	необязательные требования, несоответствие которым не оказывает значительного влияния на качество осуществления деятельности по обеспечению ИБ в рамках функционирования системы (для функциональных требований), либо не являются необходимым условием для функционирования подсистем ИБ прикладного ПО (для требований по ИБ)
2	необязательные требования, несоответствие которым не оказывает никакого влияния на качество осуществления деятельности по обеспечению ИБ в рамках функционирования системы, однако являются желаемыми для повышения эффективности работы системы

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

1. ПРОИЗВОДИТЕЛЬНОСТЬ

- Максимальное время отклика системы
- Пропускная способность
- Количество одновременных пользователей
- Масштабируемость (возможность увеличения мощности системы)

2. НАДЕЖНОСТЬ

- Время наработки на отказ
- Коэффициент готовности
- Отказоустойчивость

3. СОВМЕСТИМОСТЬ

- Совместимость с существующими операционными системами, базами данных, приложениями и оборудованием
- Поддержка стандартных протоколов и форматов данных

4. УПРАВЛЯЕМОСТЬ

- Централизованное управление системой
- Интерфейс командной строки (CLI)
- Графический интерфейс пользователя (GUI)
- Автоматизация задач
- Интеграция с системами мониторинга

5. ТРЕБОВАНИЯ К АППАРАТНЫМ И ПРОГРАММНЫМ РЕСУРСАМ

- Минимальные и рекомендуемые требования к процессору, памяти, дисковому пространству, сетевому интерфейсу
- Поддерживаемые операционные системы и версии
- Необходимое программное обеспечение

ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БАНК РАЗВИТИЯ

ТРЕБОВАНИЯ ДЛЯ ЛЮБЫХ ВНЕДРЯЕМЫХ ПРОГРАММНЫХ КОМПЛЕКСОВ как минимум содержат следующие разделы:

- идентификация и аутентификация
- управление доступом
- контроль доступа и аудит
- целостность данных и резервное копирование
- применение электронной цифровой подписи криптографических средств защиты (при необходимости)

ТРЕБОВАНИЯ ФОРМИРУЮТСЯ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМ СТБ 34 СЕРИИ И ДРУГИХ ДОКУМЕНТОВ:

указываются конкретные требования к классам защиты, мерам защиты, функциям безопасности.

ПОЛИТИКИ И ПРОЦЕДУРЫ БЕЗОПАСНОСТИ:

- система должна поддерживать реализацию политик и процедур безопасности, принятых в организации
- возможность настройки системы в соответствии с политиками безопасности.

ЗАЩИТА ОТ ИЗВЕСТНЫХ АТАК (если применимо):

- система должна быть защищена от известных атак, таких как SQL-инъекции, межсайтовый скриптинг (XSS), подделка межсайтовых запросов (CSRF) и другие.

ПРОВЕРКА БЕЗОПАСНОСТИ КОДА:

- при разработке системы при необходимости проводится проверку безопасности кода для выявления уязвимостей
- при внедрении готового программного продукта – проводится проверка на наличие уязвимостей с использованием СКЗ системы

ПРИМЕРНЫЙ СОСТАВ ТРЕБОВАНИЙ ПО ВНЕДРЕНИЮ

БАНК РАЗВИТИЯ

ТРЕБОВАНИЯ К ВНЕДРЕНИЮ КАК ПРАВИЛО ВКЛЮЧАЮТ СЛЕДУЮЩИЕ РАЗДЕЛЫ

1. Поставка или разработка проектных, эксплуатационных документов, проектов ЛНПА (при необходимости)
2. Поставка, инсталляция и настройка ПО
3. Интеграция СрЗИ с внешними автоматизированными системами и оборудованием
4. Настройка общего функционала и конфигурации системы согласно утвержденному Стандарту настроек
5. Настройка правил, инструментальных панелей (мониторов данных), активных листов (списков), фильтров и других средств, необходимых для функционирования системы, согласно заявленным требованиям
6. Требования к миграции данных (если применимо)
7. Разработка агентов (коннекторов, сборщиков) (если применимо)
8. Настройка оповещений пользователей и администраторов с использованием электронной почты и SMS-сообщений (при наличии данного функционала)
9. Настройка формирования и рассылки отчетов по расписанию/критерию, определяемому Банком (если применимо).
10. Оформление подписки (на 36 месяцев) на услуги поставщика СрЗИ (если применимо)

ПРИМЕРНЫЙ СОСТАВ ТРЕБОВАНИЙ ПО ВНЕДРЕНИЮ

ТРЕБОВАНИЯ К ВНЕДРЕНИЮ КАК ПРАВИЛО ВКЛЮЧАЮТ СЛЕДУЮЩИЕ РАЗДЕЛЫ

11. Настройку информации об активах (если применимо)
12. Подключение и автоматическое обновление через сеть Интернет репутационных баз, списков и ПО (если применимо)
13. Проведение консультаций персонала Заказчика по всем вопросам, связанным с внедрением и эксплуатацией системы, назначение лиц, ответственных за внедрение
14. Требования к опыту внедрения и квалификации работников исполнителя
15. Требования к сертификации СрЗИ и наличию лицензий у исполнителя на проводимые работы (если применимо)
16. Обучение персонала Заказчика (не менее 5-ти работников) техническому обслуживанию и эксплуатации внедряемой на авторизованных курсах
17. Сервисное обслуживание и техническая поддержка
18. Проведение опытной эксплуатации
19. Проведение испытаний системы, направленных на проверку ее готовности к вводу в промышленную эксплуатацию (согласно Программе и методике)

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ РАЗРАБАТЫВАЕМЫХ ДОКУМЕНТОВ

БАНК РАЗВИТИЯ

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

- «Техническое задание», оформленное в соответствии с требованиями, предусмотренными ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы»
- Календарный план реализации проекта (диаграмма Ганта)
- Технический проект (включая таблицу соединений и подключений, чертеж установки, план расположения оборудования) (при необходимости)
- Перечень настроек общего функционала и конфигурации программного (программно-технического) средства (далее – СрЗИ) (включая дополнительные программные (программно-технические) средства, входящие в состав поставки, а также интегрируемые с программным средством и оборудованием заказчика)
- Программа и методика испытаний

ЭКСПЛУАТАЦИОННАЯ ДОКУМЕНТАЦИЯ

- Стандарт настроек должен содержать требования к конфигурации самого СрЗИ, других систем, с которыми проводится интеграция, а также все необходимые и достаточные технологические сведения для выполнения работ по функционированию внедряемой системы
- Регламент проведения сервисного и технического обслуживания
- Руководство администратора
- Руководство пользователя и/или оператора и/или аналитика
- Техническая документация, включаемая разработчиком в стандартный комплект поставки
- Документация с описанием структуры объектов данных, состава их реквизитов и атрибутов событий, регистрируемых в журналах событий (лог-файлы, таблицы систем управления базами данных, протокол Syslog) направляемых (запрашиваемых) SIEM - системами

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ РАЗРАБАТЫВАЕМЫХ ДОКУМЕНТОВ

ПРОЕКТЫ (ШАБЛОНЫ) ЛОКАЛЬНЫХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

Дополнительно, по требованию заказчика, могут поставляться проекты (шаблоны) локальных правовых актов в объеме минимально необходимом, но при этом достаточном, для внедрения и дальнейшей постоянной эксплуатации СрЗИ

ДОКУМЕНТЫ, ПОДТВЕРЖДАЮЩИЕ ПРОВЕДЕНИЕ ВЫПОЛНЕННЫХ РАБОТ (НАСТРОЕК).

- Рабочий(е) протокол(ы) проверки выполнения инсталляции(й) СрЗИ
- Рабочие протоколы проверки выполненных настроек общего функционала и конфигурации СрЗИ
- Протокол результатов испытаний СрЗИ, направленных на выявление степени влияния указанной системы на АБС Банка.
- Протоколы завершения этапов (стадий) тестирования, приемки, включая оценку соответствия (испытаний) СрЗИ
- Протокол результатов испытаний СрЗИ, направленные на проверку готовности указанного средства к вводу в промышленную эксплуатацию
- Акт о передаче СрЗИ в промышленную эксплуатацию
- Рабочий журнал испытаний, направленных на проверку готовности СрЗИ к вводу в промышленную эксплуатацию

БАНК РАЗВИТИЯ

СПАСИБО ЗА ВНИМАНИЕ

САВИЧ Валерий Вениаминович
заместитель начальника управления - начальник отдела информационной безопасности Управления информационной безопасности и охраны