НОРНИКЕЛЬ

ВНЕДРЕНИЕ ПРИНЦИПА SECURE BY DESIGN В УПРАВЛЕНИЕ КОРПОРАТИВНЫМИ И ПРОМЫШЛЕННЫМИ ИТ-ПРОЕКТАМИ

Как мы превратили требования информационной безопасности из «головной боли» проектных команд в конкурентное преимущество металлургической компании

Москва, 2026

«ИДЕАЛЬНЫЙ ШТОРМ»: ФАКТОРЫ ДЛЯ ИЗМЕНЕНИЯ ПАРАДИГМЫ

ФАКТОРЫ

1. **Импортозамещение**
   Массовый переход на новое российское ПО и оборудование. Как следствие: уязвимости, несовместимость, отсутствие экспертизы у команд

2. **Давление сроков**
   Быстрое развитие новых технологий, экономические и другие внешние вызовы требуют быстрых решений. Задержки в бизнес-процессах неприемлемы и имеют последствия

3. **Рост угроз**
   Количество и сложность кибератак растут.
   На службе у злоумышленников и новые технологии и социальная инженерия

ПРОЕКТ ПО ВНЕДРЕНИЮ ПРИНЦИПА SECURE BY DESIGN В УПРАВЛЕНИЕ КОРПОРАТИВНЫМИ И ПРОМЫШЛЕННЫМИ ИТ-ПРОЕКТАМИ

ЦЕЛИ ПРОЕКТА:

1. Исключить срывы сроков и необходимость переделки на финальных стадиях ИТ-проектов из-за требований ИБ
2. Синхронизировать процессы: импортозамещения, вывода систем в эксплуатацию и обеспечения кибербезопасности

ЗАДАЧИ:

1. Разработать корпоративный стандарт Secure by Design для всех этапов жизненного цикла ИТ-систем
2. Создать каталог типовых безопасных архитектурных решений
3. Укрепить партнёрские отношения с проектными командами
4. Внедрить автоматизированные инструменты предпроверки решений

МЕНЯЕМ ПОДХОД К ЗАЩИТЕ: ФИЛОСОФИЯ SECURE BY DESIGN

Secure by Design

безопасность встроена в архитектуру решения с момента его создания

Раннее вовлечение — экспертиза ИБ на этапе идеи и эскиза, а не перед запуском

Экономия ресурсов — выстраивание безопасности «с нуля» дешевле, чем внедрение наложенных средств защиты

Совместное творчество — работа в одной команде с проектировщиками, поиск оптимальных решений, перевод конфликта «безопасность VS скорость» в инженерную задачу

Оптимизация процесса — отсутствие дорогостоящих переделок в конце, плавный вывод систем в эксплуатацию

ИННОВАЦИОННОСТЬ ПРОЕКТА

Уникальный для металлургической отрасли системный подход к реализации Secure by Design, масштабированный на весь портфель проектов (более 1000 ежегодно)

Переход от разовых требований к готовым типовым эскизным проектам, включающим безопасную конфигурацию 30+ компонентов

Создание автоматизированных скриптов-предпроверок — проектная команда проверяет себя до официальной приёмки, что крайне важно для промышленных ИТ

Стимул для вендоров: выявленные уязвимости (например, в программах ZVirt, eXpress и др.) устраняются в основных ветках разработки — такого уникального уровня обратной связи от заказчика в отрасли практически нет

ИСПОЛЬЗУЕМЫЕ ЦИФРОВЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ:

- Единая система согласования (цифровой след каждого проекта)
- Библиотека шаблонов для АСУ ТП, ИС, ИТСО, СППА***
- Скрипты автоматизированной проверки настроек безопасности
- База знаний по реализации требований ИБ для российского ПО и open source

***

АСУ ТП — автоматизированная система управления технологическим процессом

ИС — информационная система

ИТСО — инженерно-технические средства охраны

СППА — система противопожарной автоматики

РЕАЛИЗОВАННАЯ СТРАТЕГИЯ (ПОДХОДЫ И ЭТАПЫ)

СТРАТЕГИЯ ПРОЕКТА: ЭВОЛЮЦИОННЫЙ ПЕРЕХОД К ВСТРОЕННОЙ БЕЗОПАСНОСТИ

ЭТАПЫ

2018–2020

Формирование типовых требований ИБ, ликбез проектных команд, первые шаблоны документов

2021–2023

Разработка Стандарта ИБ, внедрение единого процесса согласования, старт пилотных проектов с Secure by Design

2024–2025

Переход на новую методику, создание типовых эскизных проектов для 4 категорий систем, запуск автоматизированных предпроверок, масштабирование на 1000+ проектов в год

КЛЮЧЕВЫЕ ПОДХОДЫ

1. Раннее вовлечение ИБ (экспертиза на стадии концепции)
2. Совместное творчество (команды ИБ + проектировщики + вендоры)
3. Безопасность как фактор скорости (отказ от «шоковых» доработок)
4. Инструментализация: шаблоны, скрипты, консультации

ИННОВАЦИОННОСТЬ ПРОЕКТА

ИБ КАК «ПОМОЩНИК»: ТРЕБОВАНИЯ И ГОТОВЫЕ РЕШЕНИЯ ДЛЯ РЫНКА

4 ИНСТРУМЕНТА, ИЗМЕНИВШИЕ ПРАВИЛА:

1. **Типовые эскизные проекты** (шаблоны): разработаны для 4 категорий систем (АСУ ТП, ИС, ИТСО, СППА). Содержат реализацию требований ИБ для более чем 30 компонентов информационных систем и АСУ ТП. Проектная команда может адаптировать уже готовый блок под текущие задачи

2. **Единый процесс согласования в одной системе.** Прозрачность статусов, предсказуемые сроки, единый цифровой след. Исключена неразбериха с почтой и версиями

3. **Автоматизированные предпроверки** (скрипты). Проектная команда может проверить себя до официальной приёмки. Снижение числа возможных неудачных итераций с доработкой

4. **Стартовые встречи и консультации.** Охвачены десятки проектных команд. Проходят обучение в компании, в т.ч. вебинары для руководителей проектов

ИБ открыта для взаимодействия и готова помогать.

ГЛАВНОЕ

Безопасная среда создаётся сразу и в правильном ключе, без лишних итераций и последующих доработок

ПОКАЗАТЕЛЬНЫЙ КЕЙС: БЕЗОПАСНОСТЬ ПОМОГАЕТ

НАША ЭКСПЕРТИЗА — ВКЛАД В УСИЛЕНИЕ БЕЗОПАСНОСТИ РЫНКА ИБ В РОССИИ

ПОКАЗАТЕЛЬНЫЕ ПРИМЕРЫ:

ZVirt — команда ИБ выявила факт хранения паролей в открытом виде → вендор устранил уязвимость не только для «Норникеля», но и для всех своих клиентов

eXprees — ряд корпоративных требований ИБ, обеспеченных при внедрении решения в Компании, были реализованы в дальнейшем и в основной версии приложения, использующегося на рынке

МЕНЯЕМ ПОДХОД К ЗАЩИТЕ — ЗАДАЕМ ВЫСОКУЮ ПЛАНКУ ДЛЯ ОТРАСЛИ

СУПЕРНИКА

ЦЕЛЬ: Разработка и внедрение супераппа — создание единой корпоративной среды для двусторонней коммуникации, доступа всех сотрудников к цифровым сервисам и новостям компании, вовлечения в повестку по ключевым вопросам бизнеса.

ПРОБЛЕМА:

Цифровая платформа, на которой планировалось развертывание супераппа (eXpress) не соответствовала корпоративным требованиям информационной безопасности

РЕШЕНИЕ:

Сформирован обширный перечень требований ИБ для обеспечения безопасности платформы. Команда проекта провела более 60 встреч, совместными усилиями выполнив в результате 198 требований ИБ

РЕЗУЛЬТАТ:

Готовое и работающее решение, в рамках которого все каналы связи, в том числе личные и групповые чаты, надежно защищены, что подтверждено успешным прохождением независимых пентестов. Обеспечена возможность безопасно подключать новые сервисы без перестройки

ТЕХНОЛОГИЧЕСКАЯ НЕЗАВИСИМОСТЬ И РАБОТА С ВЕНДОРАМИ

Поддержка вектора на импортозамещение. В основе подхода — работа с российским ПО и open source

Одним из важных аспектов принципа Secure by Design является возможность плотного взаимодействия с российскими производителями ПО и оборудования, для того чтобы обеспечить качественную и точечную проработку соответствия решений требованиям ИБ

ЭКСПЕРТИЗА ЗАКАЗЧИКА СТАНОВИТСЯ ЦЕННЫМ ВКЛАДОМ В РАЗВИТИЕ ЦИФРОВОГО СЕГМЕНТА ПРОМЫШЛЕННОЙ ОТРАСЛИ И УКРЕПЛЕНИЕ КИБРБЕЗОПАСНОСТИ

ТИРАЖИРУЕМОСТЬ

Методология и инструменты принципа Secure by Design не зависят от системы согласования проектной документации

ГОТОВЫЙ «КОРОБОЧНЫЙ» НАБОР:

- шаблоны эскизных проектов (4 категории)
- описание процессов (раннее вовлечение, стартовые встречи)
- скрипты автоматизированных проверок
- база знаний по 30+ компонентам

Тиражируемость возможна без дополнительных доработок. Актуальность и высокий уровень проработки делают данный подход оптимальным для любой сферы промышленности

МАСШТАБ И БИЗНЕС-ЭФФЕКТ

- Сокращение времени согласования с нескольких недель до нескольких дней (экономия трудозатрат проектных команд и ИБ)
- Снижение количества критических замечаний на приемочных испытаниях до единичных (исключены «шоковые доработки»)
- Предотвращение простоев производства (минимизация риска остановки производственного процесса)
- Ускорение вывода в эксплуатацию новых цифровых продуктов (четкие сроки проектных инициатив)
- Системный подход к устранению остаточных замечаниями до состояния полного соответствия требованиям ИБ (снижение рисков будущих инцидентов)
- Экономия за счёт предотвращения переделок на поздних стадиях, снижения простоев и затрат на наложенные средства защиты

ЭФФЕКТ, КОТОРЫЙ БУДЕТ ЗАМЕТЕН БИЗНЕСУ!

РЕЗУЛЬТАТЫ РАБОТЫ

1. Изменилась модель работы: ИБ вовлечена в процессы внедрения ИТ-решений «с нуля» и содействует их **ускорению и повышению качества**
2. Количество сопровождённых проектов выросло с ~200 (2019) **до 1000+ в год** (2024–2025)
3. **Время согласования сократилось** с нескольких недель до нескольких дней за счёт внедрения шаблонов и автопроверок
4. **Минимизация количества критичных замечаний** на финише проекта
5. Обеспечивается **соответствие регуляторным требованиям**
6. **Вклад в развитие** российского рынка за счет экспертизы Компании

ГЛАВНЫЙ ИТОГ

Пройден путь от подключения ИБ «в конце проекта» до гармоничного развития архитектуры безопасности «с первого дня» с учетом требований законодательства и ожиданий бизнеса