Банк «Санкт-Петербург» автоматизировал ИБ-процессы с помощью технологий российского разработчика R-Vision

Банк «Санкт-Петербург» — один из крупнейших частных банков России. На 1 апреля 2021 года в нем обслуживается 2 097 000 частных лиц и 50 000 компаний в 65 офисах в Санкт-Петербурге, Ленинградской области, Москве, Калининграде и Новосибирске, включая представительства в Краснодаре и Ростове-на-Дону. Занимает 16 место по объему активов среди российских банков (по данным информационно-аналитического агентства «Интерфакс»). Акции банка торгуются с 2007 года, включены в высший котировальный список Московской биржи с кодом BSPB.

Задачи

ИБ-специалисты Банка «Санкт-Петербург» регулярно проверяют внутреннюю систему информационной безопасности на соответствие корпоративным нормативным документам, требованиям российского законодательства и международных стандартов. Для ускорения и упрощения этой деятельности финансовой организации был необходим специализированный инструмент для автоматизации аудитов ИБ.

Кроме того, в банке решили создать собственный центр мониторинга и реагирования на киберинциденты (Security Operation Center, SOC). Поскольку команда SOC работает в круглосуточном режиме с большим потоком событий безопасности, ей понадобилась платформа для ускорения реагирования на кибератаки.

Почему R-Vision?

Специалисты Банка «Санкт-Петербург» используют технологии R-Vision с 2013 года. Тогда у кредитной организации впервые появилась потребность автоматизировать процесс проведения аудитов ИБ. Банку был необходим специализированный инструмент для выполнения проверок на соответствие Положению Банка России № 382-П, определяющему требования к защите информации при проведении денежных переводов. По результатам анализа представленных на рынке решений кредитная организация выбрала продукт R-Vision Audit Manager.

С развитием продуктовой линейки вендора и ростом потребностей банка в функциональности используемого решения в 2015 году финансовая организация решила перейти на платформу R-Vision SGRC. В то же время банк выбрал платформу реагирования на инциденты R-Vision IRP в качестве технологического ядра создаваемого SOC.

Карточка проекта

Заказчик

Банк «Санкт-Петербург»

Задачи

Автоматизация процессов управления аудитами, инцидентами ИБ, рисками

Организация взаимодействия с ФинЦЕРТ для отправки отчетов об инцидентах

Решение

Платформа управления информационной безопасностью R-Vision SGRC

Платформа реагирования на инциденты ИБ R-Vision IRP

Результаты

Систематизация и ускорение проведения аудитов ИБ

Снижение нагрузки на операторов первой линии SOC

Повышение эффективности и прозрачности ИБ-процессов

ИБ-команда выбирала решения по нескольким ключевым критериям:

- Наличие встроенных алгоритмов для управления аудитами и инцидентами ИБ;
- Поддержка российских банковских стандартов «из коробки»;
- Готовые шаблоны отчетности по инцидентам, которые легко адаптировать под себя;
- Отсутствие необходимости дорабатывать продукты самостоятельно;
- Оптимальное соотношение стоимости и функциональных возможностей продуктов.

Ход проекта

На первом этапе специалисты банка внедрили платформу SGRC. Сегодня с ее помощью они управляют всеми проверками соответствия системы информационной безопасности внутренним стандартам и требованиям регуляторов.

На втором этапе ИБ-команда банка встроила в инфраструктуру внутреннего Центра мониторинга и реагирования на инциденты платформу R-Vision IRP. На базе этого продукта был выстроен процесс инцидент-менеджмента и организовано взаимодействие с Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России — ФинЦЕРТ. С помощью системы специалисты финансовой организации отправляют регулятору отчеты об инцидентах по требованиям законодательства.

Проект в цифрах

11 500
активов оборудования обрабатывается

50+
аудитов проведено

100 000+
инцидентов в 28 категориях обработано

300+
сценариев реагирования используется

Дмитрий Бабков,
директор по информационной безопасности Банка «Санкт-Петербург»

«Нам было важно найти решение, оптимальное по стоимости и функциональным возможностям. Продукты R-Vision не требовали доработок с нашей стороны, всё необходимое мы получили «из коробки». Решения удобны и просты в установке, так как вендор предоставил нам хорошо документированные, понятные инструкции по внедрению. В пользу R-Visio сыграло и наше многолетнее сотрудничество, в течение которого компания непрерывно развивала свои продукты и делилась с нами накопленной экспертизой».

Результат

Платформа SGRC помогла банку ускорить и упростить проведение многочисленных аудитов на соответствие внутренним стандартам и законодательству.

С помощью встроенных в платформе IRP сценариев реагирования банку удалось снизить нагрузку на операторов первой линии SOC и минимизировать риск ошибок при обработке инцидентов из-за человеческого фактора.

Кроме того, платформа R-Vision используется в кредитной организации как единый инструмент для управления всеми задами по информационной безопасности. Так как все ИБ-специалисты работают в едином информационном пространстве, это обеспечивает прозрачность выстроенных процессов для каждого из них.

Планы по развитию проекта

Банк «Санкт-Петербург» непрерывно расширяет использование продуктов R-Vision с момента их запуска в промышленную эксплуатацию. В ближайших планах финансовой организации — выстроить на базе платформы SGRC систему оценки киберрисков согласно Положению Банка России №716-П. До появления специальных требований регулятора эту задачу в банке решали на основе экспертных оценок.

Кроме того, специалисты финансовой организации планируют использовать платформу R-Vision как единую мастер-систему для инвентаризации активов и автоматизировать с её помощью управление уязвимостями. Это позволит ИБ-команде не только своевременно выявлять недостатки в безопасности используемых в банке систем, но и контролировать их устранение.