КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ

В структуре Группы «Русагро» создано и функционирует Управление информационной безопасности, реализующее комплексный подход, обеспечивающий стабильную работу бизнеса путем защиты конфиденциальности, целостности и доступности информации и информационных систем.

Группа «Русагро» в своей деятельности учитывает риски кибербезопасности, в том числе риски для безопасности данных клиентов, партнеров, работников и акционеров. Группа использует современные технологии защиты, постоянно совершенствует механизмы управления киберугрозами и принимает меры по предотвращению утечек персональных и иных конфиденциальных данных.

Бизнес-ориентированная система информационной безопасности

В 2024 году в результате более шести лет сотрудничества «Русагро Тех» и АО «Инфосистемы Джет» (российский вендор решений в области информационной безопасности (ИБ)) был реализован переход Группы на бизнес-ориентированную систему ИБ.

Направления системы

- Прикладные системы защиты информации и криптографическая защита
- Мониторинг и реагирование на инциденты
- Защита сетевой инфраструктуры
- Развитие архитектуры ИБ и методологий

История развития

2017

Этап 1

Комплексный ИБ-аудит и разработка долгосрочной стратегии развития ИБ

Первичное ИБ-обследование охватило центральный офис и производственные площадки всех бизнес-направлений Группы «Русагро»: мясное, масложировое, сахарное и сельскохозяйственное. Для измерения уровня ИБ выбрали адаптированную под Группу «Русагро» модель зрелости (CMMI), которая позволяет получить унифицированную оценку уровня зрелости процессов ИБ в различных подразделениях агрохолдинга.

В стратегии были заложены механизмы контроля: ежегодный GAP-анализ изменений уровня зрелости обеспечения ИБ-процессов и оценка требуемых ресурсов, учитывающая специфику различных бизнес-направлений Компании.

Результат

В полном объеме реализована пятилетняя стратегия ИБ.

Согласно утвержденной системе оценки ИБ достигла уровня зрелости, близкого к максимальному уровню.

Аудит ИТ-инфраструктуры

16
КЛЮЧЕВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

500+
СЕРВЕРОВ

4 700
АРМ

80
КОНТРОЛЕЙ ИБ

2018–2022 →

Этап 2

Оценка процессов и модернизация

Компания «Инфосистемы Джет» ежегодно проводила оценку зрелости процессов обеспечения ИБ в Группе «Русагро» с демонстрацией результатов сравнения между прошлым и текущим годами.

Работы охватывали не только корпоративный сегмент ИТ-инфраструктуры, но и технологический – промышленные автоматизированные системы, обеспечивающие работу производственных цепочек.

15
ПЛОЩАДОК

16
ИНФОРМАЦИОННЫХ СИСТЕМ

4
ТЕХНОЛОГИЧЕСКИЕ СИСТЕМЫ (АСУ ТП)

Результат

В Компании был создан свой собственный ситуационный центр мониторинга ИБ – SOC, который занимается выявлением и реагированием на инциденты ИБ. Внедрена система мониторинга событий ИБ (SIEM) во всех бизнес-направлениях Группы «Русагро» с подключением 800 источников. На основе используемой в Компании ITSM-системы создана система управления жизненным циклом инцидентов ИБ и выстроен процесс управления инцидентами, разработаны сопутствующие документы и регламенты, введена система отчетности и систематизирован процесс взаимодействия с топ-менеджментом по вопросам инцидентов ИБ. Внедрена аналитическая платформа для анализа больших объемов данных при проведении расследований по инцидентам ИБ, что позволяет выявлять около 400–450 подтвержденных инцидентов в год.

Внедрены системы контроля привилегированных пользователей и защиты веб-приложений.

Выстроен процесс отработки запросов ИБ в адрес Департамента ИБ со стороны сотрудников Компании.

Помимо оценки зрелости процессов ИБ, ежегодно проводится анализ технической защищенности внешнего ИТ-периметра Компании и ее внутренней инфраструктуры, в том числе различных информационных систем. По итогам реализуется устранение выявленных недостатков, что позволяет значительно повышать уровень общей защищенности Компании.

Внедрена платформа автоматизации тестов на проникновение, которая моделирует логику и поведение хакера с помощью машинных алгоритмов, что позволяет тестировать защищенность инфраструктуры организации с применением новейших техник, обнаруживать слабые места в ИТ-инфраструктуре и поведении пользователей (в конце 2022 вендор ушел из России, использование системы стало невозможным).

В конце 2022 года с привлечением подрядчика в Компании реализован процесс мониторинга и блокирования мошеннических ресурсов в сети Интернет, использующих бренды Группы «Русагро» (Brand protection service), а также мониторинга и реагирования на утечки учетных записей пользователей и анализа СМИ, теневых форумов, сообществ на предмет утечек конфиденциальной информации.

2023

Этап 3

Переход Группы на систему оценки «Модель здоровья ИБ» и ежегодный ИБ-аудит

Следующей ступенью развития Компании стал переход бизнеса на систему качественных и количественных показателей.

Следуя общему бизнес-принципу, Департамент ИБ реализовал переход на систему оценки «Модель здоровья ИБ».

Модель основывается на процессном управлении ИБ, связывает показатели ИБ и ИТ-показатели с целями бизнеса. С помощью нее определяются показатели операционного и стратегического уровней для принятия правильных управленческих решений и фиксируются пороговые и целевые состояния показателей.

Результат

Ввод системы позволил построить более качественное взаимодействие со смежными функциями за счет ввода совместных показателей эффективности.

Проведено импортозамещение системы управления инцидентами ИБ (SOAR) с реализацией функционала реагирования на инциденты ИБ «по кнопке», что позволяет своевременно и безопасно (с подтверждением «второй рукой») реагировать на атаки из интернета, фишинговые почтовые рассылки и др. С помощью системы SOAR организованы сбор и обогащение данных об активах Компании (для целей ИБ), в том числе реестра опубликованных веб-приложений. Для реализации указанного функционала система SOAR интегрирована с 18 различными сторонними системами. Использование системы позволило существенно сократить время реагирования на инциденты ИБ.

После перехода на новую модель оценки зрелости ИБ – «Модель здоровья» – развитие процессов и систем ИБ продолжилось. На данном этапе:

Проведены работы по расширению зоны мониторинга инцидентов системой SIEM (общее количество источников увеличилось примерно до 1 500 шт.) и разработке внутренней логики (за годы эксплуатации разработано около 400 правил детектирования).

Требования ИБ интегрированы в процесс реализации проектов по внедрению информационных систем. Перед вводом системы в эксплуатацию в обязательном порядке проводятся работы по проверке компонентов системы на отсутствие критичных уязвимостей, постановка на мониторинг событий ИБ в SIEM, прорабатываются вопросы резервного копирования данных, планы восстановления в случае сбоя и др.

1. Аудит корреляционных правил SIEM-системы и рекомендации по их совершенствованию
2. Тестирование на проникновение веб-ресурсов и внутреннее тестирование на проникновение, тестирование Wi-Fi-сетей
3. Анализ возможности реализации недопустимых для бизнеса событий и разработка рекомендаций
4. Анализ системы обработки и защиты персональных данных

Непрерывная работа в области кибербезопасности

Тренинги и обучение сотрудников

Реализовываются регулярные мероприятия по информированию, обучению работников и повышению их осведомленности по вопросам соблюдения кибергигиены для обеспечения устойчивого иммунитета к внешнему разрушительному воздействию со стороны злоумышленников.

Архитектура ИБ

Обеспечивает структурированный подход к управлению защиты систем и сервисов, соответствующий нормативным требованиям и требованиям ИБ для обеспечения устойчивости бизнеса в условиях современных киберугроз.

Соответствие требованиям законодательства (комплаенс)

Инициированы и завершаются аудиты по оценке соответствия Группы нормативным и законодательным требованиям по замене решений зарубежного производителя на отечественные в рамках исполнения Указа Президента Российской Федерации от 1 мая 2022 года N° 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», выполнения требований Федерального закона от 27 июля 2006 года N° 152-ФЗ «О персональных данных», Федерального закона от 26 июля 2017 года N° ФЗ-187 «О безопасности критической информационной инфраструктуры» и Федерального закона от 29 июля 2004 года N° ФЗ-98 «О коммерческой тайне».

Управление рисками ИБ

Внедрена методика оценки рисков ИБ на основе использования стоимости простоя бизнес-систем и процессов, что позволяет обеспечивать разумную достаточность при принятии решений.

Управление уязвимостями

Проводятся работы по выстраиванию процесса управления уязвимостями: утверждены сопутствующие регламенты, реализован процесс ежегодного полного сканирования внешнего периметра и внутренней инфраструктуры Компании на предмет наличия уязвимостей. По результатам сканирования при взаимодействии с другими дирекциями проводится устранение выявленных недостатков.

Методология ИБ

Обеспечиваются высокая динамика и гибкость системы внутренних нормативных документов.

Проактивная защита

Для проактивной защиты от угроз реализована интеграция с общедоступной базой индикаторов компрометации, в которой аккумулируются знания о вредоносных IP-адресах, URL, доменах и т. д. С использованием SOAR перечень индикаторов угроз используется для автоматизированного формирования политик блокировки на межсетевых экранах FortiGate. Такой подход позволяет избежать большого количества потенциально опасных внешних обращений и повысить защищенность периметра Компании.