KASPERSKY lab

ПРОМЫШЛЕННАЯ КИБЕРБЕЗОПАСНОСТЬ – ЗАЛОГ УСПЕШНОГО БИЗНЕСА

История успеха

TATNEFT

Нефтяная компания

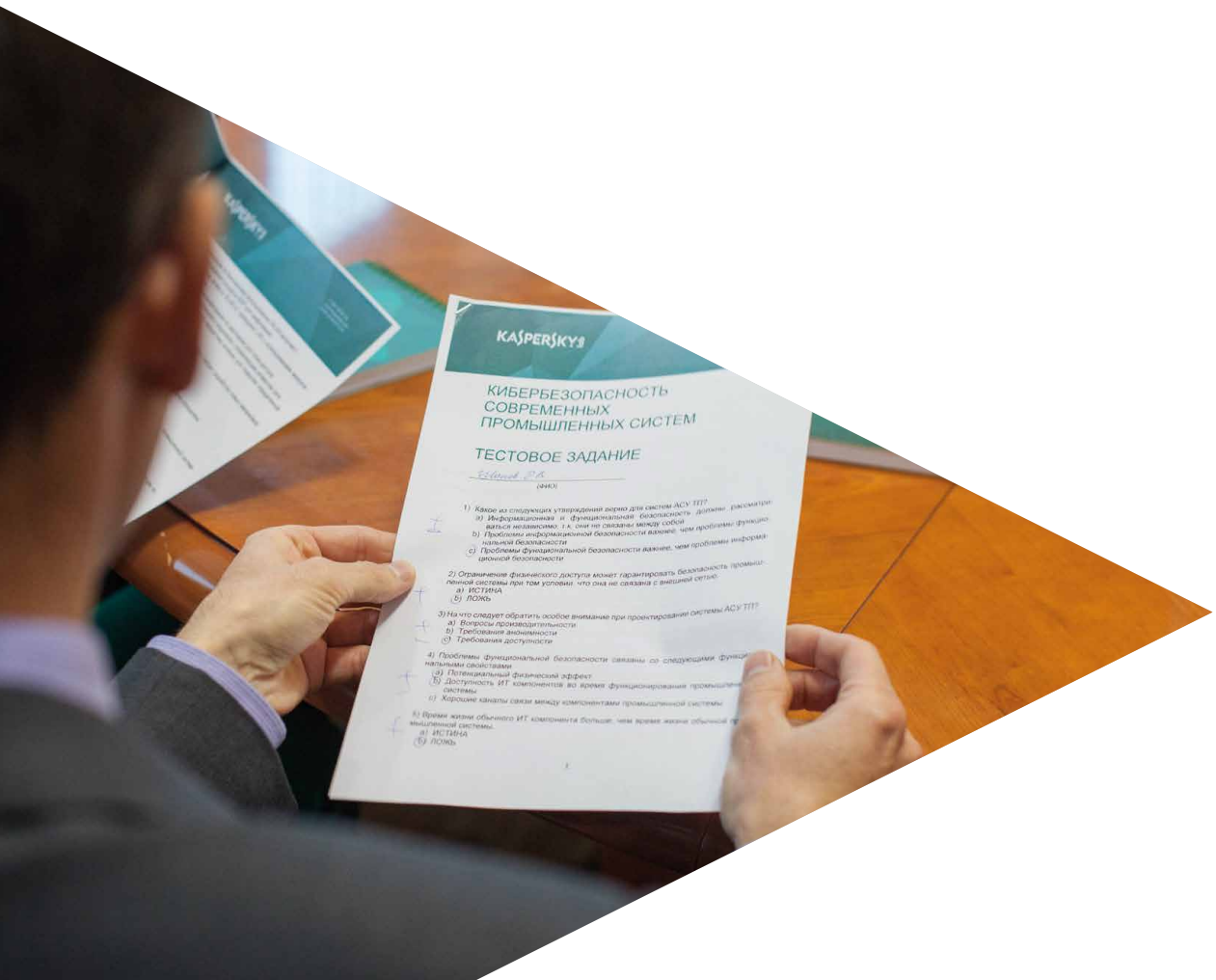
- Основана в 1950 году
- Ведет разработку более 80 месторождений нефти
- Собственные мощности по нефтепереработке и нефтехимии
- Использует Kaspersky Industrial CyberSecurity / тренинг «Кибербезопасность современных промышленных систем»

«Татнефть» – одна из крупнейших российских нефтяных компаний, вертикально-интегрированный холдинг, получивший международное признание.

В составе производственного комплекса компании стабильно развиваются нефтегазодобыча, нефтепереработка, нефтехимия, шинный комплекс, сеть АЗС и блок сервисных структур.

Добыча нефти ведется на более 80 месторождениях в разных частях России. Высокотехнологичная, эффективная и экологичная переработка нефти и выпуск конкурентоспособной продукции являются приоритетом деятельности перерабатывающих и нефтехимических производств в составе холдинга.

Нефтедобывающее и нефтеперерабатывающее производство требует тщательного подхода к безопасности, потому что инцидент не только может стать причиной сбоя внутренних процессов, но и оказать негативное влияние на окружающую среду.



Проблематика

«Обеспечение высокотехнологичной, эффективной и экологичной переработки нефти и выпуск конкурентоспособной продукции – основная задача промышленных предприятий группы компаний «Татнефть». Автоматизация технологических процессов – это один из ключевых рычагов развития бизнеса, — рассказывает начальник управления информационных технологий и заместитель главного инженера ПАО «Татнефть» Алексей Беспалов. — Передача трудоемких и высокоответственных задач автоматизированным системам управления позволяет получить технологическое преимущество и снизить затраты на производство продукции. Стратегический взгляд на развитие требует учитывать и требования безопасности, а также кибербезопасности».

«При этом при киберинцидентах риски на промышленных предприятиях гораздо выше, чем в случае домашних или даже корпоративных пользователей», — дополняет Андрей Суворов, руководитель департамента защиты промышленных и критических инфраструктур «Лаборатории Касперского».

Инциденты, вызванные киберугрозами, направленными на АСУ ТП, напрямую влияют на обычную безопасность на производстве. На территории Российской Федерации необходимость обеспечивать кибербезопасность на промышленном объекте регулируется приказом № 31 от 14 марта 2014 г. Федеральной службы по техническому и экспортному контролю. Любой автоматизированный технологический процесс является киберфизическим, и результатом этого процесса является физическое событие, поэтому киберугрозы могут привести к серьезным физическим последствиям, вплоть до нанесения вреда окружающему миру и человеку.

«В любом случае ответственность лежит на человеке, который отвечает за технологический процесс, — делает вывод Алексей Беспалов. — Поэтому те сотрудники, в обязанности которых входит следить за непрерывностью процесса и управлять связанными с ним рисками, являются ключевым элементом системы».

«Мы рассчитываем, что повышение уровня информированности о возможных сценариях угроз поможет руководителям на местах по-новому оценить возможные риски и скорректировать рабочие процессы исходя из современных требований кибербезопасности».

Алексей Беспалов,
начальник управления информационных технологий, заместитель главного инженера

Риски

В случае промышленных АСУ ТП киберугрозы могут стать причиной физического ущерба

Человеческий фактор

До 80% всех киберинцидентов на промышленных объектах происходят из-за человеческого фактора

Экспертиза

Тренинги Kaspersky Industrial CyberSecurity построены на реальном опыте расследования промышленных киберинцидентов

tatneft.ru

Kaspersky®
Industrial
CyberSecurity

Решение

Постоянно растущее число промышленных киберинцидентов по всему миру только подтверждает факт увеличивающейся доступности промышленных элементов через открытые сети и уязвимости в этих элементах, интерес хакерского сообщества к подобным объектам, активизацию кибертеррористов.

«Компания «Татнефть» выделила руководителей для участия в специализированном тренинге Kaspersky Industrial CyberSecurity. В рамках тренинга эксперты «Лаборатории Касперского» продемонстрировали возможные сценарии киберугроз, векторы атаки на промышленные объекты, поделились накопленными знаниями и практиками по предотвращению киберинцидентов, полученными в процессе анализа многочисленных инцидентов безопасности в коммерческих и государственных промышленных компаниях многих стран мира», — рассказывает Алексей Беспалов.

Важным отличием тренинга Kaspersky Industrial CyberSecurity является то, что он построен на реальных фактах и событиях, ведь в случае серьезных инцидентов безопасности или подозрений на целевую атаку эксперты «Лаборатории Касперского» призываются для анализа ситуации в организации многих стран мира. Участники тренинга имеют возможность познакомиться с глубокой экспертизой в области промышленной кибербезопасности.

«Мы рассчитываем, что повышение уровня информированности о возможных сценариях угроз поможет руководителям на местах по-новому оценить возможные риски и скорректировать рабочие процессы исходя из современных требований кибербезопасности», — говорит Алексей Беспалов.

Перспектива

Андрей Суворов из «Лаборатории Касперского» отмечает, что обучение руководителей – это только первый шаг на пути обеспечения кибербезопасности промышленного предприятия. Повышение уровня информированности приводит к пониманию дальнейших шагов по защите промышленной инфраструктуры от различных киберугроз, среди которых программы обучения для других сотрудников и внедрение специализированной киберзащиты для АСУ ТП.

Руководство компании Татнефть рассматривает возможность проведения такого тренинга и других специализированных программ обучения для сотрудников других уровней – в том числе для инженеров, отвечающих непосредственно за технологический процесс.

«Лаборатория Касперского» – наш доверенный партнер в киберпространстве, и мы рады возможности развивать наше сотрудничество в сфере защиты промышленных объектов», — подводит итог Алексей Беспалов.

kaspersky.ru/business

KASPERSKY lab