ЗАЩИТА ИНФОРМАЦИИ В ЛОГИСТИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Радченко Н.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фещенко С.Л. – старший преподаватель

В настоящее время при работе всех информационных систем возникает необходимость обеспечения заданного уровня информационной безопасности. С учетом целей и решаемых задач эта проблема становится актуальной при реализации информационных технологий в логистике.

Есть множество факторов уязвимости логистических информационных систем. Во-первых, более широкое использование операционных технологий, новых коммуникационных и беспроводных каналов, напрямую связанных с цифровыми экосистемами в логистических системах, делают компании легкой целью для хакеров. Во-вторых, это устаревшее регулирования и стандартов в области информационных технологий, недостаточная осведомленность в области кибербезопасности и, наконец, едва ли не самый существенный фактор - нехватка квалифицированных кадров, способных обеспечить защиту.

Логистические компании должны начать принимать программу кибербезопасности с оценки уровня киберзащиты в их оборудовании и программах операционных технологий и информационных технологий. Далее они могут принять меры защиты в самых важных и уязвимых приложениях и сетях. Определение областей с повышенным риском кибератак и разработка портфеля мер защиты могут быть упрощены с помощью моделей и инструментов, таких как программа управления киберрисками и их количественной оценки. Компании должны оценить свои факторы уязвимости на основе рискового подхода, где приоритет будет отдаваться вероятности и последствиям реализации киберугроз для ключевых активов. Затем можно ранжировать проекты на основе способности каждого из них повысить устойчивость с учетом затрат и, таким образом, по сути оптимизировать свои бюджеты вложений в кибербезопасность [1, 2].

После принятия этих мер предосторожности логистическим компаниям нужно сосредоточиться на реализации более комплексных концепций киберзащиты, таких как архитектура нулевого доверия. Данная методология подразумевает, что все устройства, пользователи или приложения, пытающиеся взаимодействовать с сетью, представляют собой потенциальную угрозу.

Компании могут предпринять три действия, чтобы усовершенствовать свои внутренние навыки в области кибербезопасности [3].

Во-первых, в корпоративной культуре следует перейти от невнимания к вопросам кибербезопасности к признанию острой необходимости бороться с угрозами. В каждом подразделении идея укрепления кибербезопасности по всей организации должна быть явным и ключевым аспектом.

Во-вторых, это повысить внимание к управлению киберрисками. Компании могут привлечь специалистов по кибербезопасности из университетов и частного сектора сообщив им, что у них будет возможность разработать программы киберзащиты с нуля, используя последние технологии и заменяя устаревшие системы.

Надо найти среди технологических сотрудников компании людей, которые готовы заняться инициативами в области кибербезопасности и которые продемонстрировали основные способности, необходимые успешным кандидатам. Повышение квалификации этих сотрудников и предложение им компенсации, а также меры поощрения в зависимости от должности за освоение требуемых навыков могли бы позволить логистическим компаниям быстро восполнить как минимум часть недостающей рабочей силы в кибербезопасности [4].

Однако технические проблемы – это только часть всего большого хозяйства, которое необходимо «осознать». Главный источник уязвимостей - не системы, а люди. Необходимы мероприятия по социальному инжинирингу, объяснению важности соблюдения правил информационной безопасности, регулярные тренинги и другое. Используя язык «продуктовых подходов» к информационным системам и услугам, необходимо озаботиться «встраиванием» свойств и характеристик cybersec во все сервисы и продукты, которые использует или разрабатывает организация.

Список использованных источников:

1. Безопасность логистических информационных систем : методическое пособие / В.А. Медведев. – Москва : РУСАЙНС, 2017. – 244 с.

2. Кашникова, И. В. Логистика : учебно-методическое пособие / И. В. Кашникова, С. Л. Фещенко. – Минск : БГУИР, 2019. – 92 с. : ил.

3. Сергеев В.И., Григорьев М.П., Уваров С.А. Логистика: информационные системы и технологии: учебно-практич. пособие. М.: Альфа-пресс, 2008.

4. Федоров В.В. Основы информационных технологий: учеб, пособие. М.: РИО РТА, 2006.