Янал Кілані

Дослідження впливу кібербезпеки на внутрішню діяльність організації: посередницька роль технологічної інфраструктури

Впровадження технологій у організаціях постійно супроводжується проблемами з захистом і зломами. За багато років ідея кібербезпеки стала основним об'єктом уваги багатьох організацій, які залежать від технологій у своїй діяльності, що вимагає від них приділення більшої уваги технологічній інфраструктурі. Метою дослідження є аналіз впливу факторів кібербезпеки на внутрішню діяльність організації та ролі технологічної інфраструктури у визначенні та контролі рівня захисту та кібербезпеки для внутрішньої діяльності організації. Було впроваджено кількісний підхід і використано анкетування для збору даних від зручної вибірки з 360 інженерів-програмістів, фахівців з мереж, тестувальників програмного забезпечення, веб-розробників і фахівців відділу техпідтримки за допомогою структурованого опитування. Дані було проаналізовано з використанням програми SPSS версії 21. Результати підтверджують непрямий вплив рушійних факторів кібербезпеки (зростання обсягу даних, розповсюдження технологій, доступ до необхідних ресурсів, операційний контроль, технічний контроль) на надійну внутрішню діяльність, що пояснюється стійкістю технологічної інфраструктури в організації. Фактор «зростання обсягу даних» виявився найбільш впливовим у стратегіях кібербезпеки, оскільки показав середня значення 4,2661, яке є найвищим серед усіх факторів, за ним йде фактор «технічний контроль», який показав середнє значення 4,1296. Відповідно, у статті надано рекомендації щодо розгляду організаціями інфраструктури інформаційних технологій як основної складової стратегій управління ризиками для недопущення непередбачуваних ризиків і атак.

Ключові слова: кібербезпека, зростання обсягу даних, розповсюдження технологій, операційний контроль, технічний контроль
Класифікація JEL: M15, L86

Янал Килани

Исследование влияния кибербезопасности на внутреннюю деятельность организации: посредническая роль технологической инфраструктуры

Внедрение технологий в организациях постоянно сопровождается проблемами з защитой и взломами. За много лет идея кибербезопасности стала основным объектом внимания многих организаций, зависящих от технологий в своей деятельности, что требует от них уделения большего внимания технологической инфраструктуры. Целью исследования является анализ влияния факторов кибербезопасности на внутреннюю деятельность организации и роли технологической инфраструктуры в определении и контроле уровня защиты и кибербезопасности для внутренней деятельности организации. Был внедрен количественный подход и использовано анкетирование для сбора данных от удобной выборки из 360 инженеров-программистов, специалистов по сетям, тестировщиков программного обеспечения, веб-разработчиков и специалистов отдела техподдержки при помощи структурированного опроса. Данные были проанализированы с использованием программы SPSS версии 21. Результаты подтверждают непрямое влияние движущих факторов кибербезопасности (рост объема данных, распространение технологий, доступ к необходимым ресурсам, операционный контроль, технический контроль) на надежную внутреннюю деятельность, что объясняется устойчивостью технологической инфраструктуры в организации. Фактор «роста объема данных» оказался наиболее влиятельным в стратегиях кибербезопасности, поскольку показал среднее значение 4,2661, являющееся наивысшим среди всех факторов, за ним идет фактор «технический контроль», показавший среднее значение 4,1296. Соответственно, в статье представлены рекомендации касательно рассмотрения организациями инфраструктуры информационных технологий как основной составляющей стратегий управления рисками для недопущения непредвиденных рисков и атак.

Ключевые слова: кибербезопасность, рост объема данных, распространение технологий, операционный контроль, технический контроль
Классификация JEL: M15, L86