скользкостью на автомобильных дорогах в городских условиях нежелательно. Применение таких солей на внегородских дорогах должно быть ограничено. По завершению зимнего сезона требуется периодически проводить экологические мероприятия в пределах придорожной полосы и полосе автомобильной дороги.

Учитывая проведенные исследования, можно отметить, что запасы хлорида магния составляют 250 млрд тонн и добывается он в Волгоградской области. Преимущества бишофита велики. Помимо положительного воздействия на почву, он используется как удобрение и обладает меньшей коррозионной активностью по сравнению с другими хлоридами.

Список использованной литературы:

1. Экологические проблемы строительства и эксплуатации автомобильных дорог / Под ред. Немчинова М.В. – Москва-Иркутск: 1997. – 232 с.
2. ОДМ 218.2.064-2015 Методы укрепления откосов земляного полоша автомобильных дорог засевом трав в различных климатических зонах – Введ. 2017-05-15 – М.: Росавтодор, 2017 – 69 с.
3. СП 82.13330-2016 Благоустройство территорий – Введ. 2017-06-17 – М.: Стандартинформ, 2017 – 28 с.

УДК 007

Никишина А.П.
Магистрант 2 курса КНИТУ-КАИ,
г. Казань, РФ
Научный руководитель: Базаров Р.Т.
Кандидат экономических наук, КНИТУ-КАИ,
г. Казань, РФ

БЕЗОПАСНОСТЬ В ОРГАНИЗАЦИИ

Аннотация

В статье рассмотрены подходы, с помощью которых можно начать внедрение информационной безопасности в организацию. Самое главное на этапе внедрения – поддержка высшего руководства. Без такой поддержки системные администраторы не будут иметь элементарной мотивации для того, чтобы организация была защищена от разного вида угроз. Это является важным, так как иначе компании понесут потери.

Ключевые слова

Информационная безопасность, предприятие, информационная система, подходы, информационные системы.

На данный момент увеличивается количество хакерских атак на различного рода предприятий, поэтому предприятиям необходимо защищать информацию, касательно интеллектуальной собственности, данных сотрудников и клиентов.

Безопасность должна начинаться где-то в организации, и для поддержки разнообразной программы информационной безопасности требуется широкий круг специалистов.

Даже при наилучшем планировании и внедрении невозможно обеспечить идеальную информационную безопасность. Информационная безопасность не может быть абсолютной: это процесс,

а не цель. Вы можете сделать систему доступной для любого человека, в любом месте, в любое время и с помощью любых средств. Однако такой неограниченный доступ представляет опасность для безопасности информации. С другой стороны, полностью защищенные информационные системы не позволили бы никому получить к ним доступ. Для достижения баланса, то есть для функционирования информационной системы, удовлетворяющей пользователей и специалистов по безопасности, уровень безопасности должен обеспечивать разумный доступ и в то же время защищать от угроз. [1]

Из-за современных проблем и проблем с безопасностью отдел информационной системы или обработки данных может слишком глубоко погрузиться в управление и защиту систем. Дисбаланс может возникнуть, когда потребности конечного пользователя подрываются навязчивым вниманием к защите и администрированию информационных систем.

Специалисты по информационной безопасности и конечные пользователи должны понимать, что обе группы разделяют одни и те же общие цели организации - обеспечить доступность данных, когда, где и как это необходимо, с минимальными задержками или препятствиями. В идеальном мире, этот уровень доступности может быть достигнут даже после устранения опасений по поводу потери, повреждения, перехвата или уничтожения. [2]

Внедрение информационной безопасности в организации должно с чего-то начинаться и не может произойти в одночасье. Защита информационных ресурсов - это поэтапный процесс, требующий координации, времени и терпения. Информационная безопасность может начинаться с попытки системных администраторов повысить безопасность своих систем путем совместной работы. Это часто называют подходом «снизу-вверх». Подход «снизу-вверх» - метод установления политики и/или практики обеспечения безопасности, который начинается с массовых усилий, в ходе которых системные администраторы пытаются повысить безопасность своих систем. Ключевым преимуществом подхода «снизу-вверх» является технический опыт отдельных администраторов. Работая с информационными системами на ежедневной основе, эти администраторы должны обладать глубокими знаниями, которые могут значительно способствовать разработке системы информационной безопасности. Они знают и понимают угрозы своих систем и механизмов, необходимые для их успешной защиты. К сожалению, подход «снизу-вверх» редко работает, поскольку в нем отсутствуют такие важные функции, как поддержка участников и организационная устойчивость. [3]

Нисходящий подход имеет более высокую вероятность успеха. Подход «сверху вниз» - методология разработки политики и/или практики обеспечения безопасности, инициируемая высшим руководством. При таком подходе проект формально разрабатывается и поддерживается менеджерами высшего уровня, которые разрабатывают политику, процедуры и процессы, определяют цели и ожидаемые результаты и определяют ответственность за каждое требуемое действие. Этот подход имеет сильную поддержку высшего руководства, преданного сторонника, обычно выделяемое финансирование, четкий процесс планирования и реализации, а также средства для влияния на организационную культуру. Наиболее успешный вид нисходящего подхода также предполагает формальную разработку стратегии, известная как жизненный цикл разработки систем. [3]

Чтобы любые усилия в масштабах всей организации увенчались успехом, руководство должно принять их и полностью поддержать. Роль лидера - как правило, руководителя, такого как директор по информационным технологиям или вице-президент по информационным технологиям - в этих усилиях трудно переоценить. Такой лидер продвигает проект вперед, следит за тем, чтобы им должным образом управляли, и добивается признания во всей организации. Без такой поддержки на высоком уровне многие администраторы среднего уровня не могут найти время для проекта или отклоняют его как низкоприоритетный. Участие и поддержка конечных пользователей также имеют решающее значение для успеха такого рода проектов. Пользователи самым непосредственным образом зависят от процесса и результатов проекта и должны быть включены в процесс обеспечения информационной безопасности.

Ключевые конечные пользователи должны быть назначены в группу совместной разработки приложений. Чтобы добиться успеха, такая группа совместной разработки приложений должна обладать стойкостью. Она должна быть способна выдержать текучесть кадров и не должна быть уязвима к изменениям в команде персонала, которая разрабатывает систему информационной безопасности. Это означает, что процессы и процедуры должны быть задокументированы и интегрированы в организационную культуру. Они должны быть приняты и поддержаны руководством организации. [3]

Таким образом, что начать защищать коммерческую тайну организаций, таким предприятиям необходимо знать элементарные подходы для того, чтобы начать вводить информационную безопасность в организацию. Иначе компании понесут большие потери от кражи данных, интеллектуальной собственности организации.

Список использованной литературы:

1. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.
2. Гафнер В.В. Информационная безопасность: Учебное пособие. – Рн/Д: Феникс, 2017. – 324 с.
3. Whitman M. E., Mattord H. J. Principles of Information Security/ Boston: MA 02210, 2021. 743 с.

УДК 501

Состина Е.В.
Кандидат тех. наук., доцент, ГУАП,
г. Санкт-Петербург

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ИЗГОТОВЛЕНИЯ КОМПОЗИЦИОННЫХ ЭЛЕКТРОДНЫХ ЛЕНТ

Аннотация

В статье рассмотрен вопрос автоматизации технологического производства дисперсных материалов. Охарактеризована математическая модель изготовления композиционных электродных лент. Приведены математические расчеты прочности и толщины активного слоя. Сделан вывод об экономическом аспекте производства, о внедрении «искусственного интеллекта» при дозирования фракций.

Ключевые слова

Цифровизация производства, автоматизация производства, технологии, дисперсные композиции, толщина и пористость активного слоя.

В настоящее время «цифровая трансформация» продолжает активно внедряться в различные области человеческой деятельности. Информационные технологии, искусственный интеллект переходит из раздела вспомогательных функций в основные средства технологического производства. Цифровизация химического предприятия значительно улучшит качество продукции, сократит время производства, исключает человеческий фактор и становится экономически выгодным.

Композиционные материалы широко используются в различных химических производствах. Человеческий фактор сильно ограничивает эффективность такого производства, в отличие от «искусственного интеллекта», который способен непрерывно оценивать и корректировать состав