2. Для успешного решения задач логики в СКА Maple необходимо корректно и безошибочно производить ввод логического выражения, в противном случае, результат будет неверным.

В этой связи следует отметить, что приведенные способы решения отдельных логических задач, позволяют выполнить и оценить решение логических задач, а также помогут обеспечить решение более сложных задач надисциплинах «Дискретная математика», «Математическая логика» и др.

1. Учебно-методическая разработка «Решение математических задач в Maple» // [Электронный ресурс] // URL: <https://textarchive.ru/c-1291783.html> // (дата обращения 7.05.2020).
2. Киричек К.А., Оленев А.А. Обучение бакалавров педагогического образования элементам комбинаторики с использованием информационных технологий. // Мир науки. Педагогика и психология. 2019. Т. 7. № 3. С. 9.
3. Оленев А.А., Малиатаки В.В. Моделирование логических элементов и простейших узлов ЭВМ в системе компьютерной математики Maple. // Информатика в школе. 2017. № 8 (131). С. 58-63.
4. Доказательство тавтологий // [Электронный ресурс] // URL: <https://pandia.ru/text/78/562/6568.php> // (дата обращения 10.05.2020).
5. Примеры упрощения логических формул с использованием законов логики // [Электронный ресурс] // URL: <https://multiurok.ru/files/primiery-uproshchieniia-loghichieskikh-formul-s-ispolzovaniem-zakonov-loghiki.html> // (дата обращения 11.05.2020).

Шерунтаев Д.А.

Информационная безопасность в корпоративной информационно-телекоммуникационной сети

*Владимирский государственный университет им. А.Г. и Н.Г. Столетовых
(Россия, Владимир)*

doi: 10.18411/lj-06-2020-87

idsp: ljjournal-06-2020-87

Аннотация

В данной статье рассмотрены вопросы и критерии обеспечения информационной безопасности в корпоративной информационно-телекоммуникационной сети. Рассмотрены необходимые аспекты для обеспечения информационной безопасности и их обеспечение.

Ключевые слова: Информационная безопасность, корпоративная сеть, корпоративной информационно-телекоммуникационной сети, злоумышленник.

Abstract

This article discusses issues and criteria for ensuring information security in the corporate information and telecommunication network. The necessary aspects for information security and their provision are considered.

Keywords: Information security, corporate network, corporate information and telecommunication network, attacker.

Проблема обеспечения безопасности корпоративных сетей передачи данных (КИТС) в настоящее время широко обсуждается как в отечественной науке и промышленности, так и за рубежом. Это обусловлено рядом причин, таких как:

- структурная сложность и размерность современных КИТС;
- возрастающие требования к уровню информационной безопасности (ИБ) как компонентов, так и всей КИТС, особенно предназначенных для работ на опасных промышленных объектах.

Одной из основных составляющих процесса обеспечения безопасности КИТС является локализация и устранение аномалий ее функционирования, наиболее значимыми аномалиями здесь выделим отклонения от штатного функционирования компонентов КИТС и перегрузки в каналах связи.

Таким образом, для обеспечения требуемого уровня ИБ КИТС, необходимо располагать эффективными средствами, позволяющими своевременно обнаруживать и достоверно идентифицировать инциденты ИБ, вызывающие аномалии в функционировании КИТС.

Задача обеспечения информационной безопасности (ИБ) КИТС (как частного случая технической системы) – есть одна из подзадач обеспечения ИБ предприятия. Задачи обеспечения ИБ КИТС рассматривают традиционно в общем случае в трех аспектах:

1. конфиденциальность информации, циркулирующей в КИТС;
2. целостность хранимых и передаваемых данных в КИТС;
3. доступность информации (информационных ресурсов или услуг);

Все три аспекта достаточно детально рассмотрены в современной литературе по проблемам ИБ, разработано множество эффективных моделей и методов обеспечения ИБ сетей, программно-аппаратных средств и механизмов, реализующих эти методы.

В ходе анализа по этим трем аспектам телекоммуникационных сетей, в более частном случае, информационная безопасность должна обеспечить:

- секретность (privacy, confidentiality, secrecy) персональной или уникальной информации, передающейся по КИТС, процессов ее обработки, хранения;
- целостность (data integrity) информации и обеспечение ее неизменяемости вне контроля идентифицированных операторов;
- идентификация (identification) пользователей КИТС;
- аутентификация (data origin, authentication) пользователей системы и определение его роли (ролей) в КИТС;
- уполномочивание (authorization) или допуск ролевого пользователя к определенной группе данных ;
- контроль доступа (access control) к информации в КИТС;
- права собственности (ownership) на ту или иную информацию;
- сертификация (certification) методов обработки и сервисов ;
- подпись (signature) правообладателей или отправителя информации;
- неотказуемость (non-repudiation) работы электронных сервисов и средств передачи;
- датирование (time stamping) работы с информацией, ее отправления и получения и выполнения иных информационных процессов ;
- расписка в получении (receipt) для доказательства получения информации исполнителем;
- аннулирование (annul) для отмены действия сертификатов, полномочий или подписей если ключи идентификатора оказались скомпрометированы;
- анонимность (anonymity) пользователя при совершении строго оговоренных процессов в КИТС;
- свидетельствование (witnessing) удостоверение (подтверждение) факта создания или существования информации некоторой стороной, не являющейся создателем;
- подтверждение (confirmation) истинности информации;
- ратификация (validation) процессов, методов, сервисов, отвечающим заранее установленным критериям приемлемости.

Одним из основных факторов, влияющих на эффективность функционирования КИТС является ее безопасность. Как правило, именно на КИТС приходится наибольшее количество деструктивных воздействий - естественных угроз информационной безопасности (ИБ), действий злоумышленников, халатность или некомпетентность обслуживающего персонала и пользователей, старение коммутационного и компьютерного оборудования и т.д., что влечет за собой нарушения ее (КИТС) функционирования и, как следствие, увеличение рисков ИБ предприятия.

Безопасность КИТС предприятия, согласно ГОСТ Р 52448-2005 - способность сети противодействовать определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав сети средства, линии связи и технологические процессы (протоколы), что может привести к ухудшению качества услуг, предоставляемых сетью.

В ходе анализа телекоммуникационной сети ставится возможность, согласно ранее описанным аспектам, разработка технологического алгоритма на примере алгоритма «точка-точка». Данная технология предоставит возможность быстрого, а главное безопасного соединения между устройствами в корпоративной сети передачи данных, согласно действующему ГОСТу по ИБ.

1. Система обеспечения визуальной коммуникации по защищенным каналам связи / Монахова М.М., Путинцев Г.В., Порфирьев А.А. Мазурок Д.В. // Журнал «Проблемы современной науки и образования / Problems of modern science and education». – Иваново: Изд-во «Проблемы науки», 2017, № 5. – С.31-33. ISSN 2304-2338)
2. Модульная система видеосвязи с распределенной передачей данных / Шерунтаев Д.А. Дни науки студентов Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых: сб. материалов науч.- практ. конф. 12 марта – 6 апр. 2018 г., г. Владимир [Электронный ресурс] / Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2018. – 3907 с. – ISBN 978-5-9984-0891-5 с. 203-207

Шпаковский В.П.

Интеллектуальная система оптимизации товарных потоков логистического центра

*Донской государственный технический университет
(Россия, Ростов-на-Дону)*

doi: 10.18411/lj-06-2020-88

idsp: ljjournal-06-2020-88

Аннотация

В данной статье будет исследована интеллектуальная система оптимизации товарных потоков, с использованием Интернета вещей. Насколько оптимизация логистических процессов поможет улучшить современную жизнь.

Ключевые слова: IoT, производительность, последствия, транспортировка, логистика.

Abstract

This article will explore the intellectual system of optimizing commodity flows using the Internet of things. How optimization of logistics processes will help improve modern life.

Keywords: IoT, productivity, consequences, transportation, logistics.

В 2010-х годах Интернет сделал качественный скачок вперед, и в конце десятилетия теперь предлагаются революционные цифровые решения, которые могут стать незаменимыми для любого бизнеса в будущем. Одним из таких новых