Шаханова М.В., Кий Ю.А., Шаханова В.С. Роль интернет контроль серверов в организации сетевой защиты // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 12(38) с. 11–16

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

РОЛЬ ИНТЕРНЕТ КОНТРОЛЬ СЕРВЕРОВ В ОРГАНИЗАЦИИ СЕТЕВОЙ ЗАЩИТЫ

[1]Шаханова М.В., Кий Ю.А., Шаханова В.С.
ФГБОУ ВО «МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АДМИРАЛА Г.И. НЕВЕЛЬСКОГО», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

Обеспечение сетевой безопасности является актуальной задачей на современных предприятиях, активно интегрирующих в своей деятельности информационные технологии. Цель представленной статьи заключается в анализе роли интернет контроль серверов в организации сетевой защиты применительно к области судовождения. В результате работы комплексно рассмотрены вопросы, связанные с принципом работы данной технологии, а также сформированы рекомендации по использованию различных инструментов в зависимости от условий. Практическая ценность работы состоит в возможности использования представленных материалов в качестве основы для организации сетевой защиты в организации.

Ключевые слова: Информационная безопасность, информация, интернет контроль серверов, фильтрация контента, сетевая защита.

THE ROLE OF INTERNET SERVER CONTROL IN THE ORGANIZATION OF NETWORK PROTECTION

[1]Shakhanova M. V., Kiy Yu.A., Shakhanova V.S.
MARITIME STATE UNIVERSITY NAMED AFTER G.I. NEVELSKOY, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

Ensuring network security is an urgent task at modern enterprises that actively integrate information technologies in their activities. The purpose of the presented article is to analyze the role of Internet servers in the organization of network protection in relation to the field of navigation. Because of the work, issues related to the principle of operation of this technology comprehensively considered, as well as recommendations on the use of various tools, depending on the conditions, formed. The practical value of the work consists in the possibility of using the presented materials as a basis for the organization of network protection in the organization.

Keywords: Information security, information, Internet server control, content filtering, network protection.

На сегодняшний день активно интегрируются информационные технологии практически во всех профессиональных сферах жизнедеятельности современного человека. Вместе с этим актуализируется вопрос, связанный с обеспечением защиты информации ввиду увеличения объемов электронной информации, а также используемой конфиденциальной и другой информации ограниченного доступа. Одной из таких областей является судовождение.

Актуальность вопроса информационной безопасности для данной области наблюдается сразу по нескольким причинам. Во-первых, в судовождении часто обрабатываются

конфиденциальные данные, такие как информация о пассажирах, грузе, маршрутах и другом. Нарушение безопасности этих данных может привести к серьезным последствиям, таким как утечка конфиденциальной информации или хищение личных данных пассажиров. Во-вторых, суда зависят от компьютерных систем и сетей, которые могут стать объектом кибератак. Нарушители могут попытаться проникнуть в систему судна, чтобы украсть информацию, нарушить работу систем управления или даже нанести физический ущерб.

Одним из основных способов связи и передачи информации в судовождении является использование сетей и серверов. Противоправные действия, направленные на нарушение целостности системы защиты данных способны привести к значительным негативным последствиям, вследствие чего особенную актуальность приобретает задача, связанная с обеспечением сетевой защиты в данной области.

Одним из вариантов решения данной проблемы является использование интернет контроль серверов (далее – ИКС). Данный инструмент представляет собой программный продукт, устанавливаемый на рабочий компьютер, который позволяет обеспечить контроль информационных потоков корпоративной сети и осуществляет учет трафика между сетями организации и интернетом [1]. ИКС, также называемый отечественным аналогом межсетевого экрана, позволяет организовать сетевую защиту организаций от внешних угроз и контролировать доступ пользователей за переделы сети.

На Рисунке 1 представлены все основные преимущества, наблюдаемые при использовании ИКС [2]. Важно отметить, что интернет контроль серверов является передовым отечественным решением, позволяющим обеспечить решение задач, связанных с организацией сетевой защиты.

Рисунок 1 – Преимущества ИКС в организации сетевой защиты

Работа интернет контроль серверов основана на анализе и фильтрации трафика, проходящего через него. В основе работы ИКС заложены различные алгоритмы и правила,

определяемые и индивидуально настраиваемые администратором. Именно на их основе представляется возможным определение и ограничение доступа пользователей к определенным сайтам, приложениям и иным типам контента [3]. Так, при отправлении пользователем запроса на доступ к определенному сайту или иному ресурсу происходит его перенаправление на ИКС, который, в свою очередь, анализирует заголовки запросы, содержащие информацию о протоколе, порте и адресе URL, на основе чего применяет заданные алгоритмы и правила для принятия решения о разрешении или же блокировке доступа.

Для защиты данных могут быть использованы различные способы и методы:

1. Белые и черные списки. Администратор определяет список разрешенных или запрещенных адресов URL, которые могут быть посещены пользователями. ИКС сравнивает адреса запрошенных сайтов со списками и принимает решение, разрешать или блокировать доступ;
2. Контентный анализ. ИКС анализирует содержимое запрошенных веб-страниц или файлов и применяет правила для определения наличия недопустимого или нежелательного контента, к примеру, вредоносное программное обеспечение. По результатам анализа сервер принимает решение о блокировке или разрешении доступа;
3. Контроль приложений. ИКС может анализировать сетевой трафик и определять типы приложений, используемых пользователями. Администратор может задать правила для блокировки определенных приложений или сервисов, таких как мессенджеры или социальные сети.

При этом важно отметить, что ИКС может быть индивидуально настроен для различных уровней ограничений и фильтрации в зависимости от потребностей самой организации [4]. Администратором могут быть изменены правила и параметры работы сервера в соответствии с текущими потребностями и политиками безопасности внутри организации. Зачастую выбор способа защиты зависит от масштаба организации и необходимого уровня автоматизации процессов. При использовании ИКС на небольших предприятиях достаточно использование белых и черных списков, в то время, как для средних и больших предприятий необходимо использование комплексного автоматизированного решения ИКС.

В зависимости от первостепенных задач в организации, связанных с сетевой защитой, интернет контроль серверов может применяться в качестве межсетевого экрана, системы предотвращения вторжений, защиты веб-ресурсов, контроля приложений и иных способов защиты данных [5]. Современные ИКС включают в себя сразу несколько модулей, позволяющих в отдельности или комплексно решать задачи, связанные с организацией сетевой защиты. На представленном ниже Рисунке 2 указаны основные способы защиты от несанкционированного доступа, а также внутренних и внешних угроз, реализуемые на основе интеграции ИКС в организации сетевой защиты организации.

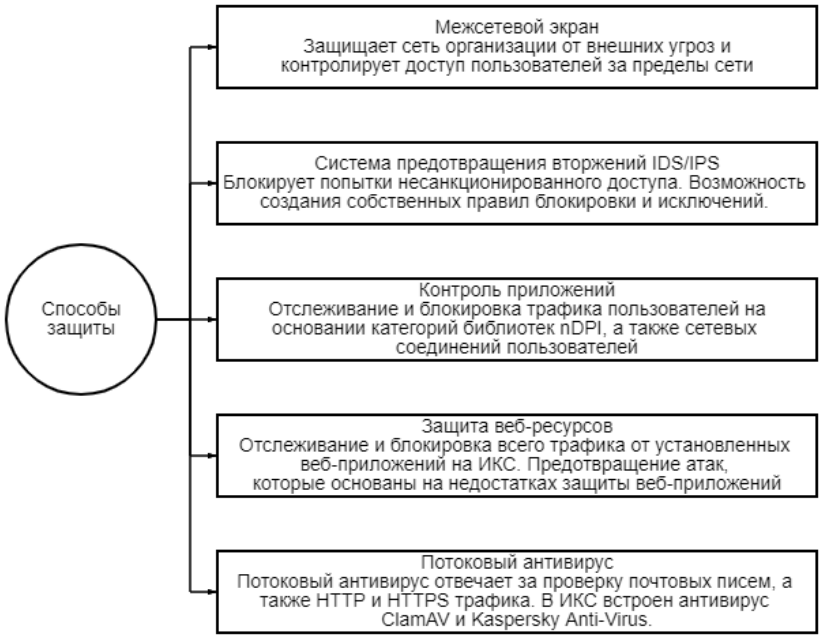

Рисунок 2 – Способы защиты в ИКС

Использование каждого из данных способов также зависит от уровня масштаба организации, используемых сетевых инструментах и необходимого уровня защиты. Основным отличием способов защиты являются решаемые задачи и применимость в зависимости от особенностей каждой определенной организации [6]. Так, к примеру, для небольших организаций, численность сотрудников которых не превышает 20 человек, достаточно использование только межсетевого экрана. При количестве сотрудников до 50 человек и решении более сложных задач необходимо использование комбинации модулей, к примеру, таких как межсетевой экран и потоковый антивирус. В более масштабных организациях, численность в которых достигает свыше 100 человек необходимо использование комбинации всех представленных на рис. 2 способов защиты интернет контроль серверов [7]. Помимо этого, выбор конкретного модуля ИКС также зависит от конкретных требований, целей и бюджета в рамках каждой определенной организации.

Интернет контроль серверов может быть интегрирован для решения различных задач. Так, к примеру, с его помощью можно обеспечить быстрый, удобный, а также безопасный обмен информацией между судном и диспетчером. Это в конечном итоге повышает эффективность принимаемых решений, увеличивая безопасность экипажа и пассажиров. Использование ИКС в данной сфере позволяет минимизировать риски, связанные с противоправными действиями и обеспечить эффективное функционирование рассматриваемой области. При этом для получения наиболее эффективных результатов важно не только выполнять регулярное обновление программного обеспечения, но и проводить аудит информационной безопасности.

Таким образом, основной целью представленной статьи являлось выполнение анализа относительно вопросов использования интернет контроль серверов в организации сетевой защиты. В результате работы определены актуальность и основные преимущества с возможностями при использовании ИКС на базе современных организаций. Выделены

основные способы защиты сетевого трафика и определены критерии использования каждого из них. В заключение необходимо отметить, что использование рассмотренных решений позволяет обеспечить высокую надежность, простоту управления и поддержки, а также устойчивость к сбоям в сетях, используемым в организациях.

Список литературы

1. Малькова Е.А. Защита информации в корпоративных сетях // Форум молодых ученых. 2019. №4 (32). С. 695-698.
2. Комилова З.Х., Назиржонова Ф.С. Методы защиты компьютерной сети от несанкционированного доступа из сети интернет // Экономика и социум. 2020. №12 (79). С. 632-634.
3. Козлова Н.Ш., Довгаль В.А. Кибербезопасность и информационная безопасность: сходства и отличия // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2021. №3 (286). С. 88-97.
4. Довгаль В.А., Довгаль Д.В. Анализ проблем обеспечения информационной безопасности беспроводных сенсорных сетей и методов обеспечения безопасности интернета вещей // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2021. №1 (276). С. 75-83.
5. Perera S., Gupta V., Buckley W. Management of online server congestion using optimal demand throttling // European Journal of Operational Research. 2020. P. 324-342.
6. Шелухин О.И., Ванюшина А.В., Габисова М.Е. Фильтрация нежелательных приложений интернет-трафика с использованием алгоритма классификации Random forest // Вопросы кибербезопасности. 2018. №2 (26). С. 44-51.
7. Певнев П. В. Система фильтрации web-трафика // Литьё и металлургия. 2022. №1. С. 89-90.

References

1. Malkova E.A. Information protection in corporate networks // Forum of Young scientists. 2019. No.4 (32). pp. 695-698.
2. Komilova Z.H., Nazirzhonova F.S. Methods of protecting a computer network from unauthorized access from the Internet // Economics and Society. 2020. No.12 (79). pp. 632-634.
3. Kozlova N.Sh., Dovgal V.A. Cybersecurity and information security: similarities and differences // Bulletin of the Adygea State University. Series 4: Natural, mathematical and Technical sciences. 2021. No.3 (286). pp. 88-97.
4. Dovgal V.A., Dovgal D.V. Analysis of the problems of ensuring information security of wireless sensor networks and methods of ensuring the security of the Internet of Things // Bulletin of the Adygea State University. Series 4: Natural, mathematical and Technical sciences. 2021. No.1 (276). pp. 75-83.
5. Perera S., Gupta V., Buckley W. Management of online server congestion using optimal demand throttling // European Journal of Operational Research. 2020. P. 324-342.
6. Shelukhin O.I., Vanyushina A.V., Gabisova M.E. Filtering unwanted Internet traffic applications using the Random forest classification algorithm // Issues of cybersecurity. 2018. No.2 (26). pp. 44-51.

7. Pevnev P. B. Web traffic filtering system // Casting and metallurgy. 2022. No. 1. pp. 89-90.