2. Ibrayev A.T., Zhunussov K., Smailov N., Tleumuratova K.T. Study of temperature sensors based on bragg grating Journal (Budapest, Hungary) The journal is registered and published in Hungary // The journal publishes scientific studies, reports and reports about achievements in different scientific fields. – 2017. – № 4. – P. 62-67.
3.Wojcic W., Жунусов К.Х., Смайлов Н.К. Исследование спектральной харектеристики оптоволоконных датчиков температуры // Вестник КазНИТУ Технические науки. – Алматы, 2016. – №1(113). – С. 293-297.
4. Варжель С.В. Волоконные брэгговские решетки. – СПб: Университет ИТМО, 2015. – С. 18-21.

БРЭГГ ТОРЫ СЕНСОРЫНЫҢ МОДЕЛІН ЖАСАУ

И.Б. Шедреева, Г.Ж. Карнакова

Брэггтың талшықты торының сипаттамаларын әзірлеу бойынша көптеген ғылыми жұмыстар бар. 100-ден астам ғылыми жұмыстар қаралды. Зерттелген ғылыми жұмыстарды негізгі қарастырылған тақырыптар мен бағыттар бойынша бірнеше үлкен топтарға жіктеуге болады: Брэгга талшықты торын құру кезінде негізгі есептерді шешу (құру әдістерін қарастырады), Брэггга торын модельдеу және Брэгга талшықты торынан сигнал сипаттамаларын зерттеу жолымен теориялық үлгіден алынған нәтижелерді практикалық нәтижелермен салыстыру.

Мақалада заңдылықтарды анықтау үшін сенсордың негізгі параметрлері келтірілген, торға енгізілген сәулелер мен кері шағылысқан сәулелер арасындағы өзара әрекеттесудің заңдылықтарын ескеру қажет. Модельді құру үшін тиімді сыну көрсеткіші, тор кезеңі, тордың ұзындығы, аподизациялық коэффициент және басқа кіріс параметрлері сияқты сенсор әзірлеушілері арасындағы негізгі параметрлерді анықтау қажет. Практикалық зерттеулер нәтижесінен тор арқылы өткен кіру және шығу сигналдарының амплитудалық мәнін анықтауға болады.

Түйін сөздер: *температура, Брэгг торы, тәуелділік, сыну көрсеткіші.*

DEVELOPMENT OF THE BRAGG LATTICE SENSOR MODEL

I. Shedreeva, G. Karnakova

There are many scientific papers on the development of characteristics of the Bragg fiber lattice. More than 100 scientific papers were reviewed. The studied scientific works can be classified into several large groups according to the main topics and directions considered: solving the main problems in creating a fiber Bragg lattice (considers the methods of creation), modeling the Bragg lattice and comparing the results obtained from the theoretical model with practical results by studying the characteristics of the signal from the fiber Bragg lattice.

The article presents the main parameters of the sensor. in order to determine the patterns, it is necessary to take into account the patterns of interaction between the rays entered into the lattice and the rays reflected back. To build a model, it is necessary to determine the main parameters between the sensor developers, such as the effective refractive index, the lattice period, the lattice length, the Apodization coefficient, and other input parameters. From the results of practical research, it is possible to determine the amplitude values of the input and output signals that passed through the grid.

Key words: *the temperature of the Bragg grating, the dependence of the refractive index.*

МРНТИ: 50.41.23

Б.Т. Ахметов[1], К.У. Зенкович[2]
[1]Алматинский университет энергетики и связи имени Г. Даукеева
[2]Университет имени Шакарима города Семей

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ МИКРОКОНТРОЛЛЕРА NODEMCU

Аннотация. *В условиях роста конкурентной борьбы, а, следовательно, и значимости информационных и телекоммуникационных технологий, особое значение приобретает задача обеспечения необходимого уровня защищенности компьютерных сетей. Существенное влияние на защищенность сети делает наличие уязвимостей. Статья посвящена результатам исследования структурных компонентов для реализации системы контроля и управления доступом (СКУД). Разработан и испытан прототип конкурентоспособной СУКД. Предложенное решение может быть реализовано с применением любого устройства, имеющего браузер и возможность подключения к беспроводной сети Wi-Fi. Разработанная СУКД не имеет аналогов на*

рынке Казахстана. Показано, что подложенный подход, в отличие от существующих, учитывает современные тенденции тотальной цифровизации бизнес-процессов на предприятии. Используя минимальные ресурсы, предприятия могут имплементировать эффективную СКУД в своих зонах защиты информационных ресурсов.

***Ключевые слова**: кибербезопасность, система контроля и управления доступом, программная реализация.*

Введение. Информационные технологии (ИТ) стали неотъемлемой частью нашей жизни и существенно влияют на успех бизнеса, его конкурентную способность как внутри страны, так и на мировой арене. По данным Департамента труда США долгосрочный рост экономики, начиная с 1948 года и в течение 50 лет, обеспечивался развитием технологий производства, однако за последние 10 лет эта роль перешла к информационным и телекоммуникационным технологиям, которые способны обеспечить более эффективное решение вопросов организации бизнес-процессов. По оценкам западных экспертов в данный момент судьба взноса ИТ в увеличение производительности труда составляет 52%.

В условиях роста конкурентной борьбы, а, следовательно, и значимости информационных и телекоммуникационных технологий, особое значение приобретает задача обеспечения необходимого уровня защищенности компьютерных сетей. Существенное влияние на защищенность сети делает наличие уязвимостей - слабых мест в системах и приложениях, использование которых злоумышленником может привести к реализации угрозы, а также неправильное конфигурирование программных и аппаратных средств, составляющих ее инфраструктуру.

Сегодня принято характеризовать такую конфигурацию, ее соответствие установленным корпоративным стандартам и политикам безопасности, термином «здоровье» (health).

Локальные пользователи и администраторы компьютерных сетей могут оценить и настроить безопасность своих систем с помощью шаблонов безопасности операционных систем (ОС) Windows, которые впервые появились в пакете обновлений Service Pack 4 (SP4) для Windows NT 4.0 [7-15]. Шаблон безопасности является текстовым файлом, содержащим параметры безопасности, его можно применить единственной командой, позволяет практически моментально настроить безопасность отдельного компьютера или сети (с помощью групповых политик в домене). Недостаток использования шаблонов заключается в том, что они не являются средством, обеспечивающим постоянный контроль безопасности системы. Единственный способ гарантировать, что параметры остаются в силе, - регулярно применять шаблон вручную или создать групповую политику, использует шаблон. Но использовать групповые политики можно только при наличии домена. Другой недостаток шаблонов заключается в том, что они позволяют оценить и настроить только параметры безопасности системы и вовсе не позволяют оценить ее защищенность: не проверяется наличие обновлений и заплаток для ОС и установленного программного обеспечения, а также не проверяется наличие антивируса и актуальность используемых сигнатурных баз.

Цель статьи: является исследование и разработка СКУД в информационно-вычислительную среду объекта информатизации, а также в помещение.

Основной материал статьи

С самого начала разработки макета встал вопрос: «Как передавать сигнал об открытии сетью?». Наш выбор остановился на локальном сервере. Его главным преимуществом является то, что он не зависит от подключения к глобальной сети. Все, что ему нужно для работы − небольшая локальная сеть, чтобы передавать данные HTTP-запросами в виде параметров. Локальный сервер реализован на базе программного обеспечения Denwer. Используются утилиты PHPMyAdmin (включающий в себя MySQL) и интерпретатор PHP 5.4.

Вся логическая часть проекта находится на сервере и написана скриптовым языком программирования PHP. Также в проекте используется JavaScript и его Фреймворк jQuery, они используются для создания уникального идентификатора пользователя и его проверки со значениями, которые находятся в базе данных. Поскольку мы имеем дело с локальным сервером, то необходимо быть подключенным к одной сети, доступ к которой нам обеспечивает роутер TP-LINK Archer C50.

Данные передаются протоколом HTTP, то есть микроконтроллер должен иметь подключение к беспроводной сети, в нашем случае обеспечивает модуль ESP-12E.

Исходя из данных потребностей, основой стал микроконтроллер NodeMCU v.1.0 Wi-Fi (ESP-12E). Он сочетает в себе компактность, встроенный модуль ESP-12E и простоту в использовании.

Микроконтроллер NodeMCU v.1.0 Wi-Fi (ESP-12E) (рис. 1).

Рисунок 1 – Питание и интерфейс подключения к ПК: Micro-USB

Технические спецификации микроконтроллера NodeMCU:
Разработчик: ESP8266 Open source Community
Тип: Одноплатный микроконтроллер
Операционная система: XTOS
Центральный процессор: ESP8266
FLASH-память: 128 kBytes
Хранилище: 4 MBytes

Схема цифровых выходов на микроконтроллере NodeMCU представлена в таблице 1.

Таблица 1 – Схема цифровых выходов на NodeMCU

I/O index	ESP8266 pin
0 [*]	GPIO16
1	GPIO5
2	GPIO4
3	GPIO0
4	GPIO2
5	GPIO14
6	GPIO12
7	GPIO13
8	GPIO15
9	GPIO3
10	GPIO1
11	GPIO9
12	GPIO10

Разработка скетча осуществлялась в программе Arduino IDE, на языке программирования C.

Плата самостоятельно сканирует все Wi-Fi сети, подключается к сети, данные которой указаны в скетчи, выводит данные о статусе подключения в COM-порт и запускает сервер, который способен обрабатывать HTTP-протокол. Программа самостоятельно обновляет данные о взаимодействии с клиентскими подключениями и сверяет аргументы, которые передаются в HTTP-протоколе.

Конечной целью в нашем макете есть зажигания светодиода. По умолчанию он горит красным, но, когда приходит сигнал о том, что «двери должны быть открытыми», светодиод начинает гореть зеленым цветом в течение пяти секунд, что символизирует размыкания электромагнитного замка.

Пользователь, впервые пытается получить доступ к объекту – сканирует QR-код необходимых дверей (рис. 2).

Рисунок 2 – QR-коды (Дверь 1, Дверь 2, соответственно)

Данные в QR-коды записаны так:

192.168.1.107/ – обращение к коренной папке локального сервера
open.php – обращение к файлу open.php
? Door = 1 – передача значения параметра door, отвечающий за ID двери
Его перенаправят на страницу, содержащую файл index.php (рис. 3)

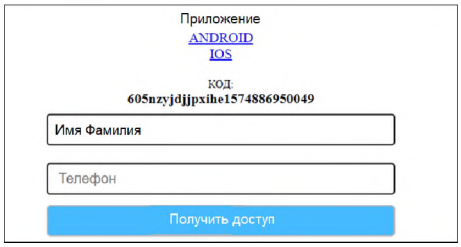

Рисунок 3 – Регистрационная форма

В браузере пользователя появляется запись cookie, содержащий уникальный идентификатор пользователя (код). На этой странице пользователь указывает свои персональные данные и нажимает кнопку «Получить доступ». После чего создается запрос в локальную базу данных, право предоставить доступ пользователю имеет только администратор.

Панель администратора представлена на рисунке 4:

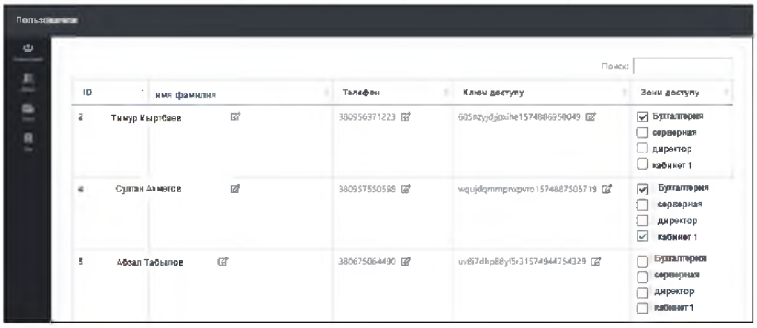

Рисунок 4 – Панель администратора

В QR-коде, привязан к двери, находится запрос в файл open.php, который обрабатывает данные с cookies и проверяет доступ пользователя к зоне.

Если пользователю разрешен проход в данную зону, то происходит перенаправление на файл success.php, который в свою очередь создает HTTP-запрос методом POST на микроконтроллер NodeMCU, или сообщает об ошибке в случае, если в пользователь не имеет права прохода в данную зону.

Контроллер сверяет аргумент, который находится в запросе и если все правильно, то плата зажигает зеленый цвет светодиода.

Все действия, совершенные авторизованными пользователями, записываются в базу данных в виде коротких логов с пометкой времени, что делает процесс мониторинга намного легче.

В среднем для идентификации одного пользователя требуется 3 секунды с момента сканирования QR-кода и к зажиганию светодиода, что свидетельствует о высокой пропускной способности созданной системы (тесты проводились в браузере Google Chrome). Это значение зависит от быстродействия устройства и установленного браузера.

Безопасность системы не подлежит сомнению. Все данные, находящиеся на сервере – защищены от SQL-инъекций, панель администратора защищена паролем, а запрос на плату осуществляется с передачей трех параметров (если в системе наглядно несколько дверей, то параметров – 4), данные о которых находятся на сервере.

При прямом обращении к локальному серверу или плате, пользователь перенаправляет на другие страницы.

Поскольку основой проекта является веб-сайт, то нам удалось создать удобный рабочий интерфейс, используя базовые средства разработки (см. рис. 5).

Логирование в нашем макете реализовано очень практично и лаконично.

Рисунок 5 – Лог

Было проведено исследование скорости работы программы и сервера в самых популярных браузерах на разных платформах: персональный компьютер и смартфон. Результаты представлены на рисунке 6.

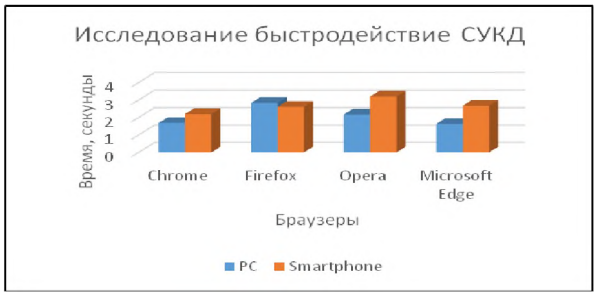

Рисунок 6 – Сравнение быстродействия СУКД на компьютере и смартфоне

В среднем выполнения полного цикла программы занимает больше времени при работе со смартфона.

Скорость выполнения зависит от качества Интернет подключения и браузера, а именно его версии и количества кэша, cookies.

Скорость удовлетворительная при использовании любого браузера из вышеупомянутых, код работает исправно.

Выводы

Результатом проведенного в рамках статьи исследования является решение проблемных вопросов, связанных с разработкой и внедрением системы контроля и управления доступом (СУКД) в условиях тотальной цифровизации.

В результате проведенного исследования сформулированы следующие выводы и предложения:

1. СКУД – чрезвычайно эффективное средство поддержания безопасности на различных объектах цифровизации. Автоматизация контроля позволяет сократить расходы на охрану и охранные пункты, позволяет поднять рентабельность предприятия, а без нее сетевого варианта трудно представить работу многих корпораций. Таким образом, внедрения СКУД – это очень выгодная инвестиция в будущее предприятия.

2. Разработан и испытан прототип конкурентоспособной СУКД. Предложенное решение может быть реализовано с применением любого устройства, имеющего браузер и возможность подключения к беспроводной сети Wi-Fi. Разработанная СУКД не имеет аналогов на рынке Казахстана.

3. Предложенный подход, в отличие от существующих, учитывает современные тенденции тотальной цифровизации бизнес-процессов на предприятии. Используя минимальные ресурсы, предприятия могут имплементировать эффективную СКУД в своих зонах защиты информационных ресурсов.

Литература

1. Абрамов А. М. Системы управления доступом. [Текст]: учебн. пособ. / А.М. Абрамов, О.Ю. Никулин, А.И. Петрушин. – М.: «Оберег-РБ», 1998.

2. Ворона В. А. Системы контроля и управления доступом. [Текст]: учебн. пособ. / В.А. Ворона, В.А. Тихонов. – М.: Горячая линия «Телеком», 2010.

3. Гинце А. Новые технологии в СКУД [Текст] /А. Гинце // Системы безопасности. – 2005. – № 6. – С. 21.
4. Злотник Е. Touch Memory – новый электронный идентификатор [Текст] / Е. Злотник // Монитор. – 1994. – №6. – С. 28-32.
5. Мальцев И. В. Системы контроля доступом[Текст] / И.В. Мальцев // Системы безопасности. – 1996. –№ 1. –С. 43-45.
6. Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Eenterprise Technologies, (1(2)), pp. 4-15.
7. Arendt, D. L., Burtner, R., Best, D. M., Bos, N. D., Gersh, J. R., Piatko, C. D., & Paul, C. L. (2015, October). Ocelot: user-centered design of a decision support visualization for network quarantine. In Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on (pp. 1-8). IEEE.
8. Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D., & Fernando, A. (2016, January). Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model. In Consumer Electronics (ICCE), 2016 IEEE International Conference on (pp. 502-503). IEEE.
9. de Carvalho, M. A., & Bandiera-Paiva, P. (2017, October). Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri Nets (CPN) modeling. In Security Technology (ICCST), 2017 International Carnahan Conference on (pp. 1-8). IEEE.
10. Appel, M., Konigorski, U., & Walther, M. (2018). A Graph Metric for Model Predictive Control of Petri Nets. IFAC-PapersOnLine, 51(2), pp. 254-259.
11. Gao, Z., Zhao, C., Shang, C., & Tan, C. (2017, October). The optimal control of mine drainage systems based on hybrid Petri nets. In Chinese Automation Congress (CAC), 2017 (pp. 78-83). IEEE.
12. Narayanan, M., & Cherukuri, A. K. (2018). Verification of Cloud Based Information Integration Architecture using Colored Petri Nets. International Journal of Computer Network and Information Security, 10(2), 1.
13. V. A. Lakhno, Y. N. Tkach, T.A. Petrenko, S.V. Zaitsev, V.M. Bazylevych. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks, Eastern-European Journal of Enterprise Technologies, No 6/9 (84), 2016, pp. 32-44.
14. G. Beketova, B. Akhmetov, A. Korchenko, V, Lakhno, A. Tereshuk. Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition. Computer modelling and new technologies, Vol. 21, No. 2, 2017, pp. 7-16.
15. Lakhno V., Petrov Al., Petrov Ant. Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport, Information Systems Architecture and Technology: 38th International Conference on Information Systems Architecture and Technology (ISAT 2017), Wroclaw, 17-19 September 2017 : proceedings, Wroclaw : Springer, 2017, pp. 113-127.

NODEMCU MICROCONTROLLER-ГЕ НЕГІЗДЕЛГЕН ҚОЛ ЖЕТІМДІЛІКТІ БАСҚАРУ ЖҮЙЕСІН ДАМЫТУ

Б.Т. Ахметов, К.У. Зенкович

Өсіп келе жатқан бәсекелестік жағдайында және, демек, ақпараттық және телекоммуникациялық технологиялардың маңыздылығында компьютерлік желілердің қажетті қауіпсіздігін қамтамасыз ету міндеті ерекше орын алады. Осалдықтар желінің қауіпсіздігіне айтарлықтай әсер етеді. Мақала қол жеткізуді басқару және басқару жүйесін (АБЖ) енгізуге арналған құрылымдық компоненттерді зерттеуге арналған. Бәсекеге қабілетті SDMS прототипі жасалды және сыналды. Ұсынылған шешім браузері бар және сымсыз Wi-Fi желісіне қосылу мүмкіндігі бар кез келген құрылғыны қолдана отырып жүзеге асырылуы мүмкін. Әзірленген СМЖ-нің Қазақстан нарығында баламасы жоқ. Жалған тәсіл, қолданыстағыдан айырмашылығы, кәсіпорындағы бизнес-процестерді жалпы цифрландырудың қазіргі тенденцияларын ескеретіні көрсетілген. Минималды ресурстарды қолдана отырып, кәсіпорындар ақпараттық ресурстарды қорғау аймақтарында тиімді АБЖ енгізе алады.

Түйін сөздер: *киберқауіпсіздік, қол жеткізуді басқару және басқару жүйесі, бағдарламалық қамтамасыздандыру.*

DEVELOPMENT OF ACCESS CONTROL SYSTEM BASED ON NODEMCU MICROCONTROLLER

B. Akhmetov, K. Zenkovich

In the context of growing competition, and, consequently, the importance of information and telecommunication technologies, the task of ensuring the necessary level of security of computer networks is of particular importance. Vulnerabilities make a significant impact on network security. The article is devoted to the study of structural components for the implementation of access control and management system

(ACS). A prototype of a competitive SDMS was developed and tested. The proposed solution can be implemented using any device that has a browser and the ability to connect to a wireless Wi-Fi network. The developed QMS has no analogues in the market of Kazakhstan. It is shown that a forged approach, unlike the existing ones, takes into account current trends in the total digitalization of business processes in the enterprise. Using minimal resources, enterprises can implement effective ACS in their protection zones of information resources.

Key words: *cybersecurity, access control and management system, software implementation.*

МРНТИ: 50.41.23

Б.Т. Ахметов[1], Д.Т. Курушбаева[2]
[1]Алматинский университет энергетики и связи имени Г. Даукеева
[2]Университет имени Шакарима города Семей

МОДЕЛЬ АДАПТИВНОГО УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА В СЕТИ

Аннотация: *Описана концептуальная модель адаптивного управления киберзащитой информационно-вычислительной сети (ИВС). Рассмотрен пример решения задачи адаптивного управления правами доступа пользователей с использованием аппарата сетей Петри. Реализована соответствующая модель и выполнено имитационное моделирование в пакетах PIPE v4.3.0 и Petri.Net Simulator. 2.017. Как и любой объект информатизации ИВС требует решения задач по защите информации и кибербезопасности (КрБ). Общей первоначальной задачей при построении эффективных систем защиты и КрБ ИВС ОБИ, остается задача обследования конкретного объекта защиты, формирование моделей потенциального нарушителя (компьютерного злоумышленника – КЗЛ) и киберугроз. По мнению большого числа специалистов, достаточно перспективным представляется возможность описания функциональных моделей различных систем защиты ИВС в терминах теории сети Петри. Реализация вышеуказанных шагов позволит в конечном итоге получить адекватные требования к системам защиты информации (СЗИ) ИВС ОБИ.*

Ключевые слова: *кибербезопасность, защите информации, сеть Петри, киберугроза.*

Введение. Современный уровень применения информационных технологий (ИТ) и систем (ИТС) в экономике достиг высочайшего уровня. При этом, появился новый термин – информационно-вычислительная сеть объекта информатизации (ИВС ОБИ).

В условиях усложнения сценариев кибератак аналитикам служб информационной безопасности (ИБ) необходимо достаточно оперативно реагировать на кибератаки, аномалии угрозы. Это делает актуальной задачу поиска новых способов повышения результативности принятия решений в заданиях реагирования на попытки деструктивного вмешательства со стороны КЗЛ или недобросовестного персонала в работу объектов информатизации, в том числе, ИВС.

Такое представление позволит аналитикам ИБ и ЗИ детализировать киберугрозы в ИВС. Кроме того, в последующем, возможно определение состояний, которые потенциально определяют уязвимости ИВС перед новыми киберугрозами. Также рассматривается перспективность применения данной модели основе сетей Петри (и Петри-Маркова) и раскрашенных сетей Петри в качестве математической и алгоритмической составляющих, проектируемой интеллектуализтрованной системы поддержки принятия решений (ИСППР) в процессе анализа кибеугроз для ИВС.

Основываясь на работах, модели угроз возможно построить, используя достаточно наглядную табличную форму отображения угроз при актуализации вопроса оценки защищенности ИВС. Но как было указанно ранее, данный подход к составлению моделей угроз трудоемок.

Сети Петри (и Петри-Маркова) успешно использовались и для описания моделей нарушителя. Однако, авторы не рассматривали возможность корректировки модели нарушителя (КЗЛ) в ИВС, в частности путем объединения ее с моделями на основе теории графов, что позволило бы более точно описать переходы состояний в процессе вероятного преодоления КЗЛ периметров (рубежей) киберзащиты ИВС.

В работах, также предлагались модели, основанные на сетях Петри и описывающие процессы реализации угроз в информационных системах (ИС). И ходя данные модели