Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Трещев Иван Андреевич
Treschev Ivan Andreevich
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»,
факультет компьютерных технологий, каф. ИБАС
«Komsomolsk-on-Amur state technical University, faculty of computer technologies
Заведующий каф. ИБАС
the head of the Department of information security of automated systems and
Кандидат технических наук
E-Mail: kalkT@yandex.ru

Григорьев Ян Юрьевич
Grigoriev Jan Yurievich
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»,
факультет компьютерных технологий, каф. ВМ
«Komsomolsk-on-Amur state technical University, faculty of computer technologies
Доцент кафедры Высшая математика
Associate Professor of the chair of Higher mathematics
Кандидат физико-математических наук/доцент
E-Mail: Jan198282@mail.ru

Воробьев Антон Александрович
Vorob'ev Anton Alexandrovich
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»,
факультет компьютерных технологий, каф. ИБАС
«Komsomolsk-on-Amur state technical University, faculty of computer technologies
Аспирант каф. ИБАС
post-graduate student of the Department of information security of automated systems and
E-Mail: zeromem@mail.ru

Система защиты конфиденциальной информации для высших учебных заведений «Электронный университет»

The confidential information protection system for higher educational institutions «Electronic University»

Аннотация: В данной статье рассматриваются вопросы, связанные с обеспечением информационной безопасности предприятий на примере высшего учебного заведения. Рассматривается комплексный подход к построению системы защиты персональных данных сотрудников, контрагентов и другой конфиденциальной информации циркулирующей на предприятии.

The Abstract: This article discusses the issues related to provision of information security of the enterprise on an example of a higher educational institution. Is devoted to the complex approach to construction of systems of protection of personal data of employees, counterparties and other confidential information circulating at the enterprise.

Ключевые слова: Защита информации, персональные данные, электронный университет, межсетевой экран, шифрование, безопасность данных, информационная система, персональные данные.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Keywords: Protection of information, personal data, electronic University, firewall, encryption, data security, information system, personal data.

***

Введение

В настоящее время законодательная база РФ в области защиты информации определила не только понятие конфиденциальной информации(КИ), но и методы, способы и средства обеспечения состояния ее защищенности[1]. Законодательство становится ориентированным на электронный документооборот(ЭДО) на предприятии. Выработать обобщенный подход к построению системы комплексной защиты информации на предприятии возможно лишь в самых общих чертах. Это связано в первую очередь с тем, что структура каждого предприятия уникальна, причем уникальна не только организационная структура, схема локальной вычислительной сети(ЛВС), сети электропитания, заземления уникально и расположение мест обработки информации подлежащей защите в соответствии с законодательством. Практически каждое предприятие в нашей стране имеет подключение к глобальной открытой сети обмена данными – Internet. Большая часть угроз безопасности КИ связана с возможным проникновением злоумышленников в ЛВС предприятия[2]. В работе авторами рассматривается построение системы защиты информации, при организации информационного обмена посредством глобальной сети Internet, для высшего учебного заведения планирующего или осуществляющего переход на возможность работы со студентами, сотрудниками и заказчиками посредством открытых сетей обмена данными, с учетом обрабатываемой в ВУЗе КИ.

Министерство образования и другие ведомства внедряют разного рода информационные системы(ИС), в которых необходим обмен информацией посредством открытой глобальной сети Intenet, поэтому необходимо защищать информацию, обрабатываемую в автоматизированных системах (АС), находящихся на территории предприятия.

Общие сведения

Взаимодействие с открытыми сетями и структура ЛВС каждой ИС обобщенно может быть представлено в виде следующей диаграммы см. рис. 1.

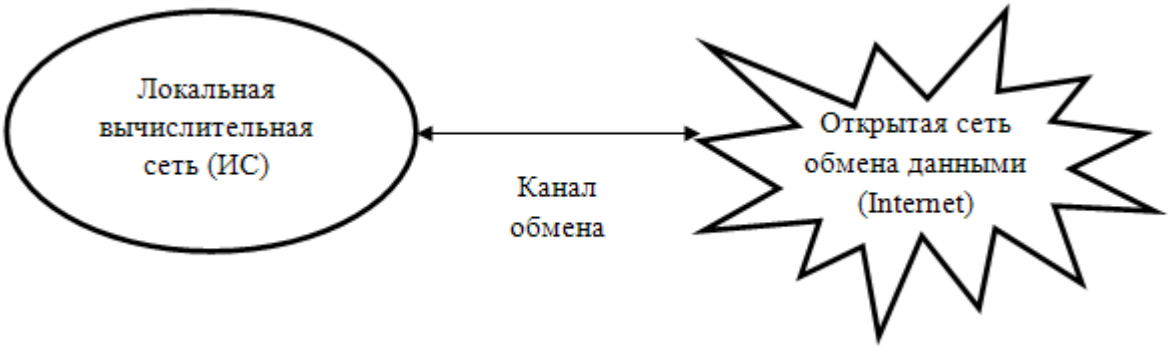

Рис. 1. *Обобщенная схема взаимодействия*

Ясно, что в случае, когда вся обрабатываемая предприятием информация может быть отнесена к категории общедоступной, то и построение системы защиты не вызывает трудностей. В случае ВУЗа, наоборот, очевидно, что обрабатываемые данные сотрудников, студентов и заказчиков являются КИ и подлежат защите в соответствие с действующим

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

законодательством. Сверх того, на любом предприятии есть подразделения обрабатывающие коммерческую тайну (в случае ВУЗа - бухгалтерия), которая так же подлежит защите.

Пусть количество студентов – N, количество преподавателей P и количество контрагентов Q, тогда сумма $N+P+Q$ превышает для типового ВУЗа 1 000, для крупных ВУЗов эта величина превышает 10 000. Конечно, можно говорить, что учреждение обрабатывает КИ без использования средств автоматизации и выполняет все требования Роскомнадзора по обеспечению безопасности персональных данных(ПДн), но в настоящее время авторам не известны случаи, когда в организации в отделе кадров не установлен был бы персональный компьютер, и на нем не велась бы обработка данных. В силу выше сказанного любую информационную систему ВУЗа необходимо классифицировать в соответствии с действующими нормативно-методическими документами (НМД), как информационную систему персональных данных (ИСПДн) класса не ниже К2, что влечет за собой обязательные требования по защите информации от несанкционированного доступа(НСД), экранированию определенных сегментов ЛВС предприятия, защите от утечек по техническим каналам, наличию организационно-распорядительной документации (ОРД), применению средств криптографической защиты информации(СКЗИ)[3].

В данной работе авторами рассматриваются вопросы организации ЛВС предприятия, применения средств защиты информации от НСД(СЗИ НСД), применению межсетевых экранов(МЭ).

Стоит отметить, что каждая организация по своему уникальна и предложенные подходы могут не в полной мере быть применимы для них.

Отметим, что с точки зрения защиты информации, в случае, если в организации используется беспроводная сеть передачи данных WiFi, без использования СКЗИ построить систему защиты отвечающую требованиям НМД и требований по обеспечению состояния защищенности АС и ЛВС не представляется возможным, поскольку обеспечить блокирование передачи за пределы контролируемой зоны(КЗ) не представляется возможным.

Под контролируемой зоной в данной работе понимается охраняемая территория предприятия. С точки зрения минимизации затрат на СЗИ, оптимальный вариант построения ЛВС предприятия и сопряжения ее с ГОСИБ – это выделение отдельной, единственной точки подключения к ГОСИБ и размещение ЛВС предприятия в пределах КЗ.

Немаловажным процессом при организации системы защиты ВУЗа, как и любого другого предприятия, является минимизация затрат на систему защиты информации (СЗИ), причем этот процесс не должен приводить к существенному затруднению работы пользователей.

Отметим, что организация СЗИ это по принципу Парето лишь 20% от общего числа работ по обеспечению состояния защищенности информации в ВУЗе, 80% работ приходится на внедрение и сопровождение системы защиты.

Анализ возможных подходов к организации системы защиты

В настоящее время существуют два диаметрально противоположных подхода к организации СЗИ на предприятии.

Первый заключается в выделении отдельных мест для доступа к КИ, циркулирующей на предприятии и организация работы подразделений таким образом, что при необходимости внесения данных в ИС пользователю необходимо прийти на специально выделенное для этого автоматизированное рабочее место (АРМ). Так же при использовании такой схемы выделяют отдельные места для доступа к открытым сетям информационного обмена, зачастую места

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

для доступа к ИС находятся в отдельном помещении, как и места для доступа к глобальным сетям. Данный подход, безусловно, является самым экономически выгодным с точки зрения затрат на СЗИ.

Второй же заключается в том, что каждое АРМ пользователя ИС и каждое место доступа к открытым сетям подлежит защите. С точки зрения пользователей организации этот метод является наиболее удобным, но с точки зрения затрат осуществление мероприятий по защите КИ является весьма дорогостоящим.

Для ВУЗа, с учетом необходимости оптимизации затрат на СЗИ, наиболее приемлемым является комбинированный метод, заключающийся в том, что необходимо экранировать определенные подразделения от внешних воздействий, организовать доступ к ИС и к открытым сетям для АРМ пользователей только лишь при необходимости.

Анализ ЛВС

Для высшего учебного заведения после определения перечня информации подлежащей защите, следует в первую очередь определить места обработки КИ. Для типового ВУЗа можно предложить следующий обобщенный перечень:

1. Бухгалтерия.
2. Деканат.
3. Кафедра.
4. Отделы и подразделения, отвечающие за сопровождение учебного процесса.
5. Другие отделы и подразделения.
6. Руководство университета.
7. Руководители структурных подразделений.
8. Подразделения не взаимодействующие с ИС и с ГОСИБ.
9. Подразделения(АРМ) не взаимодействующие с ИС, но взаимодействующие с ГОСИБ.
10. Удаленные рабочие места в Internet.

Отдельное выделение 6 и 7 пунктов перечня вызвано тем, что для данных мест является характерным необходимость как доступа к ИС предприятия, так и к глобальным открытым сетям информационного обмена(ГОСИБ).

Отметим, что в рамках пунктов 1-5 аналогично есть необходимость доступа к ГОСИБ, но с точки зрения минимизации затрат на СЗИ представляется возможным подключение к ИС предприятия всех пользователей и организация выделенных мест для работы с ГОСИБ.

В перечне не выделены учебные лаборатории, поскольку подключение их к единой информационной системе ВУЗа не является обязательным, а скорее даже приведет к увеличению стоимости работ по организации СЗИ.

В настоящее время немыслима информационная система,доступ к которой не возможен посредством ГОСИБ, поэтому необходимо в СЗИ предусмотреть возможность подключения пользователей посредством всемирной сети Internet, с обязательным шифрованием траффика содержащего КИ.

В силу вышесказанного определим 5 типов рабочих мест, на которых может обрабатываться КИ:

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

1. Имеющие подключение к ИС организации, но не имеющие подключения к ГОСИБ.
2. Имеющие подключение к ГОСИБ, но не имеющие подключения к ИС организации.
3. Имеющие подключение как к ГОСИБ, так и к ИС организации.
4. Не имеющие подключения к ИС организации и к ГОСИБ.
5. Удаленные рабочие места в ГОСИБ.

Для каждого типа рабочих мест определим категории средства защиты, использование которых необходимо:

1. СЗИ от НСД, антивирус.
2. СЗИ от НСД, антивирус, система обнаружения вторжений(СОВ).
3. СЗИ от НСД, антивирус, СОВ, МЭ.
4. Антивирус.
5. СЗИ от НСД, антивирус, система обнаружения вторжений(СОВ), МЭ, клиент для шифрования.

Определим соответствие между местами обработки КИ, рабочими местами и категориями средств защиты см. табл. 1.

Таблица 1

Распределение средств защиты

Место обработки КИ	Тип рабочего места	Категория средств защиты
1	1	1
2	1	1
3	1	1
4	1	1
5	1	1
6	3	2
7	3	2
8	4	4
9	2	3
10	5	5

Удаленные места обработки КИ в ГОСИБ должны удовлетворять не только требованиям по программной защите, но и требованиями от утечек по техническим каналам.

Анализ рынка средств защиты

На рынке программного и программно-аппаратного обеспечения защищенности КИ существует довольно много продуктов в той или иной степени удовлетворяющие требованиям НМД.

Последние изменения документов по антивирусной защите, необходимо наличие единого центра для обновления и управления программного обеспечения и наличие брэндмауэра, поэтому авторам представляется возможным применение на территории университета антивирусов Касперского и DrWebпоследних редакций.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Относительно МЭ в настоящее время существуют три компании –«ИнфоТекс», «Код безопасности», «Амикрон», продукты которых находят широкое применение в организациях различной формы собственности.

Отметим, что в качестве МЭ можно использовать любой сертифицированный Федеральной службой по техническому и экспортному контролю (ФСТЭК РФ) по определенному классу в соответствии с руководящими документами ФСТЭК РФ, например, VipNetOfficefirewall, ФПСУ/IP, Connectraи другие.

В качестве сервера доступа(СД) можно использовать любой сертифицированный по требования Федеральной службы безопасности (ФСБ РФ) по определенному классу крипто средств (КС), например VipNetHW 100/1000, ФПСУ/IP, АПКШ Континент и другие.

В качестве СЗИ от НСД можно использовать любое сертифицированное по требованиям ФСТЭК РФ по определенному классу, например,DallasLock, Страж NT, Аккорд и другие.

В качестве СОВ можно использовать любую сертифицированную по требованиям ФСТЭК РФ по определенному профилю Форпост, Аргус, Рубикон, Континент EndPointProtection.

Внедрение электронного правительства в РФ будет основано на продукции компании ИнфоТекс, с другой стороны у данного разработчика отсутствуют продукты СЗИ от НСД и СОВ, поэтому взаимодействие в рамках информационной системы электронный университет, по мнению авторов, нужно строить на базе продуктов «Код безопасности». В настоящее время данная компания выпускает продукты по всем основным направлениям защиты КИ на предприятии (исключая организационно-техническую документацию и защиту от утечек по техническим каналам).

С точки зрения авторов перечень в соответствии с категориями средств защиты введенными ранее, является наиболее подходящим по соотношению цена/качество/исполнение требований законодательства:

1. СЗИ от НСД – ПАК Соболь совместно с SecretNet.
2. Антивирус – DrWebилиSecurity Studio Endpoint Protection Antivirus.
3. СОВ - Security Studio Endpoint Protection HIPS.
4. МЭ –либо АПКШ континент(что представляется авторам весьма дорогостоящим решением), либо один из межсетевых экранов компании «Инфотекс».
5. СД – АПКШ ЦУС Континент.
6. Клиент для СД(клиент для шифрования) – Континент АП.

Практический опыт внедрения, установки и настройки средств защиты свидетельствует, что оптимальный вариант комбинации различных средств – это использование программного обеспечения одного производителя на всей площадке предприятия. Вопросы совместимости программного обеспечения выходят за рамки данной работы.

Рекомендуемая схема построения инфраструктуры университета с учетом требований по информационной безопасности

С учетом рекомендаций приведенных в табл. 1 и разграничения при помощи МЭ можно предложить следующую схему ЛВС ВУЗа и подключения его к ГОСИБ см. рис. 2.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

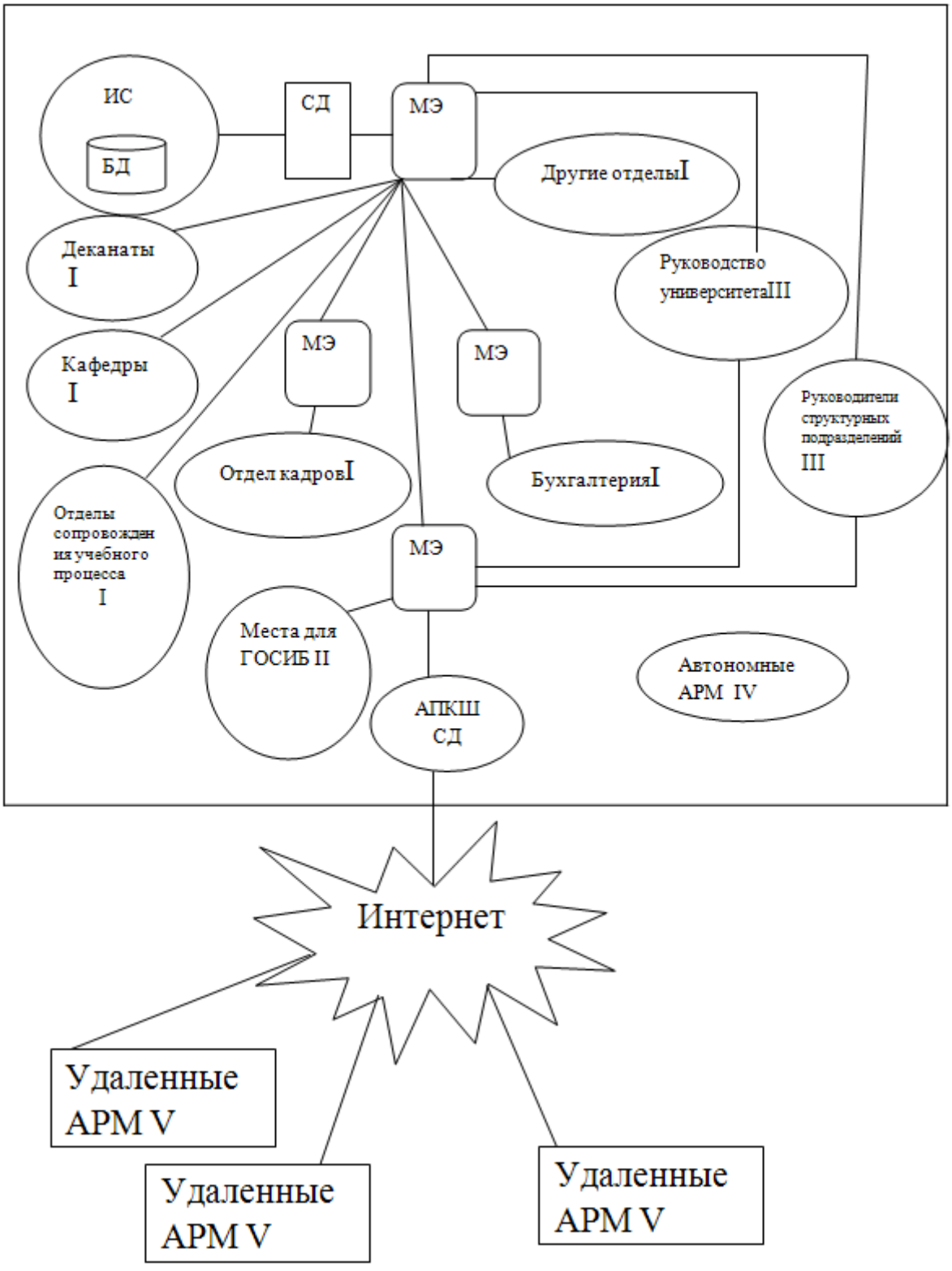

Рис. 2. *Схема ЛВС предприятия и структура СЗИ*

Несомненным достоинством данной схемы является, то, что потенциальный злоумышленник располагаясь в ГОСИБ должен преодолеть СД и один МЭ для доступа к ЭВМ в ЛВС и два СД и два МЭ для доступа к Базе данных. Если же будет проводиться «инсайдерская атака» на ИС предприятия, то в этом случае нужно преодолеть как минимум один МЭ и один СД. Существенных недостатков несколько: сложная настройка оборудования, довольно высокие затраты на СЗИ. Но указанные недостатки не снижают

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

ценность предложенного подхода, поскольку использование сертифицированных средств защиты позволяет предполагать, что атаки злоумышленников будут существенно затруднены.

Например, применение СД позволяет затруднить атаку распределенного перебора[5], поскольку используются современные алгоритмы шифрования, аутентификации и идентификации пользователей.

Заключение

В работе рассмотрены вопросы организации работы с внутренней сетью предприятия посредством открытых сетей обмена данными. Рассмотрены подходы к построению защищенных каналов обмена информацией, применения наложенных средств защиты от несанкционированного доступа. В качестве примера предприятия рассматривается высшее учебное заведение, но все указанные методы, способы и средства можно применять и в произвольных организациях при соответствующей модификации.

Комплексная система защиты информации должна включать помимо рассмотренных мер еще и систему контроля доступа на территорию предприятия, организационные меры, принятые для противодействия потенциальным злоумышленникам, средства защиты информации от утечек по техническим каналам[4].

Планируется дальнейшее исследование вопросов, не рассмотренных в данной работе в связи с ужесточением требований законодательства в области ЭДО, обеспечения состояния защищенности конфиденциальной информации, применения новых средств защиты.

ЛИТЕРАТУРА

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. Гриф Министерства образования и науки. – М.: Горячая линия-Телеком, 2006. – 544 с.: ил. ISBN 5-93517-292-5.

2. Воробьев А.А. Алгебраические методы исследования таксономий уязвимостей вычислительных сетей и компьютерных систем/ Доклады ТУСУРа 1(25), часть 2, ISSN 1818-0442, С 12-15.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебник для вузов. Под ред. Зайцева А.П. и Шелупанова А.А. Гриф министерства образования и науки РФ. – 7-е изд., испр. и доп.- М.: Горячая линия - Телеком, 2012.- 425 с.: ил. ISBN 978-5-9912-0084-4 .

4. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Монография. – Томск: Изд-во В-Спектр, 2007.- 278 с.: ил.

5. Трещев И.А. Оценка временных затрат для осуществления распределенного перебора в гетерогенных системах при помощи временных волновых систем //Доклады ТУСУРа 1(25), часть 2, ISSN 1818-0442, С. 141-148.

Рецензент: Биленко Сергей Владимирович, доктор технических наук, доцент ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет» Помощник ректора по информатизации учебного процесса