Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 005.92

На правах рукописи

КАЛИНОВСКАЯ
Анастасия Александровна

РАЗРАБОТКА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ПРИМЕРЕ ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

АВТОРЕФЕРАТ
диссертации на соискание степени

магистра технических наук

по специальности 1-38 80 04 – Технология приборостроения

Минск 2019

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **КУНКЕВИЧ Дмитрий Петрович,**
кандидат технических наук, доцент кафедры «Системы автоматизированного проектирования» учреждения образования «Белорусский национальный технический университет»

Рецензент: **ГОЛУБОВА Ольга Сергеевна,**
Кандидат экономических наук, заведующая кафедрой «Экономика, организация строительства и управление недвижимостью» учреждения образования «Белорусский национальный технический университет»

Защита диссертации состоится «26» июня 2019 г. года в $9^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 408, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

В течение последних десяти лет наметился переход от традиционной формы представления документации к электронным документам.

Переход к электронному документообороту несет целый ряд преимуществ. Прежде всего, введение электронных документов позволит существенно сократить сроки разработки и прохождения новых документов в структуре учреждения, упростить работу по формированию и пересылке пакетов документов между организациями и территориально распределёнными офисами одного предприятия.

Использование систем электронного документооборота (СЭД) послужит фундаментом для формирования единого информационного пространства организации. Введение электронных архивов позволит значительно сократить бумажный архив любого предприятия и обеспечит возможность быстрого поиска и представления электронных копий документов. Предполагается также ощутимая экономическая выгода.

Основу для создания защищённого документооборота организации сегодня видят по-разному: одни – в повышении эффективности нормативно-правовых мер защиты информации, другие – в повышении эффективности технических мер по защите информации.

Защищённая система электронного документооборота должна обеспечивать сохранность и подлинность документов, безопасный доступ и протоколирование действий пользователя в условиях потенциальных угроз информационной безопасности.

Существующие механизмы обеспечения защиты информации не в состоянии решить ряд специфических задач характерных для электронного документооборота. В частности использование открытых ключей каналов связи для предоставления, передачи и распространения электронных документов чревато возможным перехватом документов третьей стороной. Основными задачами являются защита аппаратных средств и прочих устройств подсистем СЭД; защита сетевой среды, в которой функционирует СЭД, а также каналов передачи данных и сетевого оборудования.

Эффективным способом защиты является создание системы управления информационной безопасностью, которая является современным процессом обеспечения безопасности информационных ресурсов организации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

На сегодняшний день в Республике Беларусь переход от бумажного документооборота к электронному для всех организаций и учреждений установлен на законодательном уровне. В связи с этим подготовлена и опубликована законодательная база, регулирующая документационное обеспечение управления, делопроизводство, электронный документооборот и сферу его обращения.

Система электронного документооборота несет в себе значительное количество преимуществ, в том числе сокращение времени обработки документов и экономическую выгоду за счёт большого количества факторов.

Информационные системы относятся к ряду основных защищаемых элементов учреждения образования. Обеспечение безопасности информации в системе электронного документооборота является одной из ключевых задач при построении работы всего программного комплекса учреждения. Особенно остро встаёт вопрос о защите информации на текущем этапе, по причине того, что почти вся системообразующая информация учреждения хранится и передаётся в электронном виде.

Появление новых программных продуктов приводит к активному развитию средств негативного воздействия и несанкционированного доступа к информации систем электронного документооборота. С учётом этого персоналу необходимо непрерывно анализировать угрозы и совершенствовать способы защиты информации в СЭД.

Разработка комплексной системы защиты, учитывающей все направления защиты системы электронного документооборота является актуальной.

Научная новизна исследования заключается в совершенствовании теоретических положений, разработке оригинальных методов и моделей систем технической защиты электронных документов.

Степень разработанности проблемы

Для раскрытия темы диссертации были рассмотрены: Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи», Закон Республики Беларусь «Об информации, информатизации и защите информации», Закон Республики Беларусь «Об электронном документообороте», учебные справочники по делопроизводству, материалы научных конференций и семинаров, научно-практический иллюстрированный журнал «Архивы и делопроизводство».

Одним из недостатков исследований, представленных в современной

литературе, является неполное рассмотрение способов и методов защиты информации в системах электронного документооборота. Предложенное исследование направлено на дополнение методов и способов защиты электронных документов.

Цель и задачи исследования

Целью диссертации является разработка комплексной системы защиты электронного документооборота на примере технического университета, а также разработка методов совершенствования защиты информации в СЭД.

Поставленная цель работы определяет следующие основные задачи:

1. Провести анализ архитектуры системы электронного документооборота учреждения образования

2. Дать характеристику угрозам и атакам, совершаемым на систему электронного документооборота. Классифицировать методы и средства защиты информации в автоматизированных системах.

3. Исследовать основные принципы построения защиты информации в СЭД. Дать характеристику реализации комплексной системы защиты электронного документооборота.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 80 04 «Технология приборостроения».

Теоретическая и методологическая основа исследования

В диссертационной работе были применены основы информатики и документоведения, методы информационной безопасности, методы программирования, а также анализ нормативных правовых актов по рассмотренной тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных источников, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в том, что в результате исследования разработана комплексная система защиты электронного документооборота.

Теоретическая значимость работы заключается в детальном анализе методов обеспечения защиты информации электронного документооборота с

учётом характеристики угроз и атак СЭД.

Практическая значимость состоит в разработке системы защиты электронного документооборота, которая позволит увеличить безопасность СЭД высшего учебного заведения.

Основные положения, выносимые на защиту

1. Методика оценки эффективности систем защиты информации СЭД с учётом требований информационной безопасности.
2. Метод и принципы построения системы защиты СЭД.
3. Комплексная система защиты электронного документооборота на базе SMBusiness.

Апробация диссертации и информация об использовании её результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 55-ой юбилейной научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2019 г.).

Публикации

Изложенные в диссертационной работе основные положения и выводы опубликованы в 4 печатных работах. В их числе 2 статьи в сборниках материалов научных конференций.

Общий объём публикаций по теме диссертационной работы составляет 8 авторских листа.

Структура и объём работы

Диссертация состоит из введения, общей характеристики работы, трёх глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе проанализированы требования к организации защиты электронного документооборота.

Во второй главе проанализированы угрозы информации систем электронного документооборота.

В третьей главе представлена реализация комплексной защиты системы электронного документооборота.

В приложении представлены публикации автора и регламент функционирования СМДО государственный органов Республики Беларусь.

Общий объём диссертационной работы составляет 102 страниц. Из них 65 страниц основного текста, иллюстраций на 5 страницах, таблицы на 3 страницах, библиографический список из 55 наименований на 6 страницах,

список собственных публикаций соискателя из 4 наименований на 1 странице, 4 приложения на 25 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы защиты информации в СЭД. Совершен обзор существующих методов и средств защиты информации в СЭД, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

В **общей характеристике** работы показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В **первой главе** приведен обзор архитектуры систем электронного документооборота (рисунок 1). Дана характеристика состояния проблемы защиты информации в СЭД. Описаны сущность, принципы и функциональность системы электронного документооборота БГУИР.

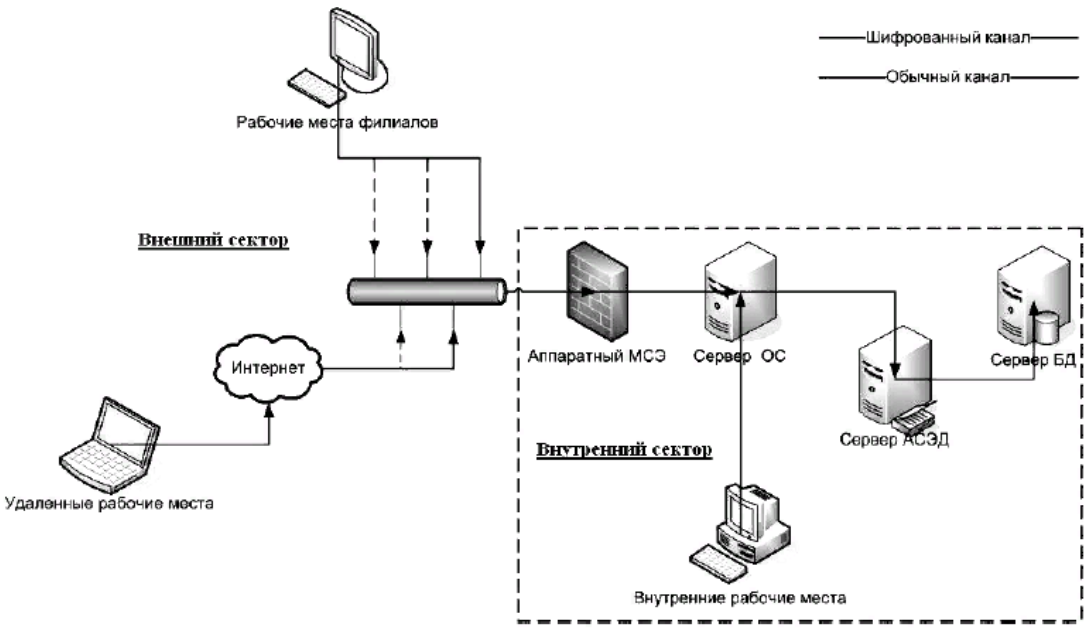

Рисунок 1 – Общая модель СЭД

Система электронного документооборота включает в себя три типа компонента, которые показаны на рисунке 1:

1. Серверы.
2. Рабочие места.

3. Каналы связи

Классифицированы основные угрозы информации в системах электронного документооборота, такие как:

1. Остановка функционирования системы в результате некорректных действий администратора СЭД;

2. Получение информации о специфике организации документооборота в организации;

3. Получение несанкционированного доступа к электронному документообороту, выполнение присвоения чужого пользовательского идентификатора;

4. Уязвимость системы к различного рода атакам преднамеренного характера;

5. Перехват трафика.

Во **второй главе** рассмотрены общие требования к безопасности системы электронного документооборота. Дана характеристика классификации угроз и атак, совершаемых на СЭД.

Совершен обзор существующих методов и средств защиты информации в системах электронного документооборота.

На рисунке 2 изображена схема степени ценности компонентов СЭД с точки зрения обеспечения целостности хранимой информации.

Рисунок 2 – Степень ценности компонентов СЭД

Объектами данной угрозы могут быть все компоненты СЭД, такие как:

– *документы*. Данные, хранящиеся на сервере баз данных, резервные копии документов. Так как именно сами документы содержат информацию конфиденциального характера, данное звено является самым важным. Для безопасности которого организована вся система политики безопасности

автоматизированной системы электронного документооборота.

– *сервер базы данных*. Среда хранения электронной документации;

– *сервер операционной системы и автоматизированной системы электронного документооборота.* Операционная система и интерфейсная часть (оболочка) системы электронного документооборота, установленные на серверах и рабочих станциях, включая клиентов СУБД, протоколы передачи данных.

Следует также учесть, что при внештатных ситуациях в рамках этих компонентов частично или полностью могут быть нарушены транзакции информации внутри СЭД, компоненты отнесены к сектору №.3.

В **третьей главе** приведен обзор программного продукта «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP» (Криптопровайдер AvCSP).

Как показывает практика, применение организационных и технических мер обеспечивает наиболее полную защиту системы электронного документооборота.

К инженерным мероприятиям относятся:

– охрана помещений с ПК и аппаратными средствами СЭД;

– сигнализация;

– защита акустического сигнала;

– экранирование помещений.

К техническим мероприятиям, в свою очередь относятся использование физических, аппаратных, программных и криптографических средств защиты системы электронного документооборота.

Инженерно-технический элемент системы защиты включает в себя:

– сооружения физической защиты от проникновения посторонних лиц на территорию, в здание и помещения;

– средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализации, информирования и идентификации);

– средства противопожарной охраны;

– технические средства контроля, предотвращающие вынос персоналом из помещений специально маркированных предметов, документов, дискет, книг.

Взаимосвязь рассмотренных выше мер обеспечения безопасности приведена на рисунке 3.

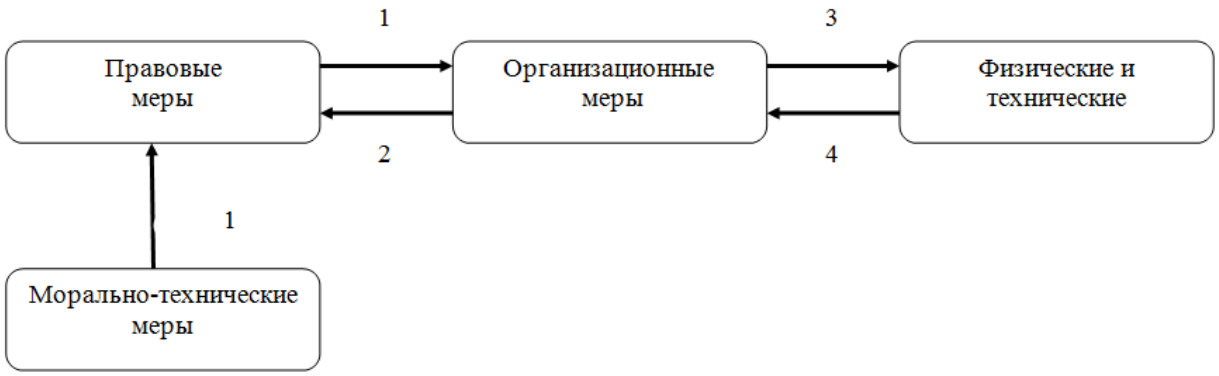

Рисунок 3 – Взаимосвязь мер обеспечения безопасности

1 – Организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации;

2 – Воплощение организационных мер требует создания нормативных документов;

3 – Для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами;

4 – Применение и использование технических средств защиты требует соответствующей организационной поддержки.

По результатам проведенного анализа возможных угроз автоматизированной системы можно сформулировать перечень основных задач, которые должны решаться системой компьютерной безопасности:

– управление доступом пользователей к ресурсам АС с целью ее защиты от неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного (с превышением предоставленных полномочий) доступа к ее информационным, программным и аппаратным ресурсам со стороны посторонних лиц, а также лиц из числа персонала организации и пользователей;

– защита данных, передаваемых по каналам связи;

– регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;

– контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы;

– контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;

– обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему

потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов;

– управление средствами системы защиты.

Выявленными принципами построения системы защиты СЭД являются:

– принцип системности;

– принцип комплексности;

– принцип непрерывности защиты;

– принцип разумной достаточности;

– принцип гибкой системы защиты.

Принцип системности. Системный подход к защите компьютерных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности автоматизированной системы.

Принцип комплексности. В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем.

Принцип непрерывности защиты. Защита информации – это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Разумная достаточность. Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности.

Гибкость системы защиты. Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты.

Предприятием, выступающим инфраструктурным оператором важнейших межведомственных информационных систем, поставляющих фундамент электронного правительства в Республике Беларусь, является Национальный центр электронных услуг (НЦЭУ).

Инфраструктура открытых ключей (Public Key Infrastructure) – один из важнейших элементов криптографической подсистемы развитой информационной системы. Она представляет собой систему программных и/или аппаратных средств, должностных инструкций (политик и регламентов), позволяющих субъектам документооборота (абонентам информационной системы) обмениваться открытыми ключами, получать достоверную информацию о владельцах открытых ключей, их полномочиях, проверять достоверность этой информации, управлять доверием абонентов друг к другу.

Программа AvPCK используется совместно с программой «Персональный менеджер сертификатов Авест» и является логическим компонентом инфраструктуры открытых ключей системы криптографической защиты информации (СКЗИ) и, совместно с программой «Центр цифровых сертификатов Авест», обеспечивает организацию системы доверия к открытым ключам участвующих в обмене электронными документами пользователей.

Программа Avest Personal CryptoKit создает удобный пользовательский интерфейс для выполнения криптографических операций шифрования данных, их подписи и проверки корректности ЭЦП.

Применение отдельных компонентов в качестве единой комплексной системы защиты даёт хороший результат.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Изучены нормативно-правовые документы, служащие основание для ведения делопроизводства и электронного документооборота в Республике Беларусь.

2. Проведен анализ арихитектуры системы электронного документооборота учреждения образования..

3. Дана классификация основных угроз и атак на систему электронного документооборота учреждения. Характеризованы методы и средства защиты информации в автоматизированных системах.

4. Проанализирована архитектура и принципы построения системы защиты СЭД.

5. Реализована защита информации на примере системы электронного документооборота SMBusiness.

Рекомендации по практическому использованию результатов

На основании результатов исследований возможно построение комплексной системы защиты электронного документооборота, которая будет удовлетворять современным стандартам информационным безопасности.

Полученные результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в лекционный курс «Управление проектами»

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в рецензируемых журналах

1. Защита центра обработки данных от угроз безопасности / Калиновская А.А., Савицкая Д.Г., Мигалевич С.А. // Электронный научный журнал «Вестник современных исследований». – Омск: Научный центр «Орка» выпуск №6-18 от 28 июня 2019 с.39 ISSN 2441-83003.

2. Основные угрозы системы электронного документооборота / Калиновская А.А. // Электронный научный журнал «Вестник современных исследований». – Омск: Научный центр «Орка» выпуск №3-18 от 27 марта 2019 с.39 ISSN 2441-83003.

Тезисы *конференций*

3. Анализ существующих методов и средств обеспечения безопасности информации и виртуализации в высшем учебном заведении / А.А. Калиновская, Д.Г. Савицкая // Материалы 55-ой юбилейной международной конференции аспирантов, магистрантов и студентов БГУИР, Минск, Респ. Беларусь, 24-29 апреля 2019 г. / УО БГУИР. – Минск, 2019.

4. Внедрение системы электронного документооборота в высшем учебном заведении / А.А. Калиновская // Материалы 54-ой международной конференции «Развитие науки в 21 веке», Харьков, Украина, 17-20 февраля 2019 г. / Науч.-исслед. центр «Знание». – Харков, 2019.

РЭЗЮМЭ

Каліноўская Анастасія Аляксандраўна

Распрацоўка комплекснай сістэмы абароны электроннага дакументазвароту на прыкладзе тэхнічнага

Ключавыя словы: бяспека, электронны дакументаабарот, СЭД

Мэта працы: распрацоўка комплекснай сістэмы абароны электроннага дакументазвароту на прыкладзе тэхнічнага універсітэта, а таксама распрацоўка метадаў удасканалення абароны інфармацыі ў СЭД.

Атрыманыя вынікі і іх навізна: выкананы дасканалы аналіз інфраструктуры існуючай сістэмы электроннага дакументазвароту вышэйшай навучальнай установы, які паказаў што электронны дакументаабарот пабудаваны на СЭД SMBusiness.

Вывучаны нарматыўна-прававыя дакументы, служачыя падстава для вядзення справаводства і электроннага дакументазвароту ў Рэспубліцы Беларусь. У ходзе даследаванняў вызначылася, што нарматыўна-прававая база па дадзенай галіны развіваецца паэтапна. Прааналізаваныя вартасці і недахопы сістэм электроннага дакументазвароту, дзе галоўным недахопам у такіх сістэмах з'яўляецца інфармацыйная бяспека. Дана класіфікацыя асноўных пагроз і нападаў на сістэму электроннага дакументазвароту ўстановы. Вызначаны асноўныя групы метадаў і сродкаў абароны інфармацыі ў сістэмах электроннага дакументаабароту. Была зроблена выснова, што пад час выкарыстаньня сучасных сістэм электроннага дакументазвароту варта ўжываць у комплексе вышэйапісаныя групы метадаў і сродкаў абароны інфармацыі. Разгледжаны асноўныя патрабаванні для сістэм электроннага дакументазвароту ў цэлым, і вызначаны дадатковыя патрабаванні для абароненых сістэм электроннага дакументаабароту. Прааналізавана архітэктура і асноўныя прынцыпы пабудовы сістэмы абароны СЭД. Рэалізаваная абарона інфармацыі на прыкладзе сістэмы электроннага дакументазвароту SMBusiness.

Ступень выкарыстання: Атрыманыя вынікі ўкаранёны ў навучальны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі» у лекцыйны курс «Кіраванне праектамі».

Вобласць ужывання: установы вышэйшай адукацыі.

РЕЗЮМЕ

Калиновская Анастасия Александровна

Разработка комплексной системы защиты электронного документооборота на примере технического

Ключевые слова: безопасность, электронный документооборот, СЭД

Цель работы: разработка комплексной системы защиты электронного документооборота на примере технического университета, а также разработка методов совершенствования защиты информации в СЭД.

Полученные результаты и их новизна: выполнен доскональный анализ инфраструктуры существующей системы электронного документооборота высшего учебного заведения, который показал что электронный документооборот построен на СЭД SMBusiness.

Изучены нормативно-правовые документы, служащие основание для ведения делопроизводства и электронного документооборота в Республике Беларусь. В ходе исследований определилось, что нормативно-правовая база по данной отрасли развивается поэтапно. Проанализированы достоинства и недостатки систем электронного документооборота, где главным недостатком в таких системах является информационная безопасность. Дана классификация основных угроз и атак на систему электронного документооборота учреждения. Определены основные группы методов и средств защиты информации в системах электронного документооборота. Был сделан вывод, что при использовании современных систем электронного документооборота следует применять в комплексе вышеописанные группы методов и средств защиты информации. Рассмотрены основные требования для систем электронного документооборота в целом, и определены дополнительные требования для защищённых систем электронного документооборота. Проанализирована архитектура и основные принципы построения системы защиты СЭД. Реализована защита информации на примере системы электронного документооборота SMBusiness.

Степень использования: Полученные результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в лекционный курс «Управление проектами».

Область применения: учреждения высшего образования.

SUMMARY

Kalinovskaya Anastasia Alexandrovna

Development of an integrated electronic document protection system based on the example of technical

Keywords: security, electronic document circulation, EDS

The object of study: to develop an integrated system for protecting electronic document management using the example of a technical university, as well as developing methods for improving information security in the EDMS.

The results and novelty: a thorough analysis of the infrastructure of the existing electronic document management system of the higher educational institution was carried out, which showed that the electronic document management system is built on the SMBusiness EDMS.

We studied the legal documents that serve as the basis for record keeping and electronic document circulation in the Republic of Belarus. In the course of the research it was determined that the regulatory and legal framework for this industry is developing in stages. The advantages and disadvantages of electronic document management systems are analyzed, where the main disadvantage of such systems is information security. The classification of the main threats and attacks on the institution's electronic document management system is given. The main groups of methods and means of information protection in electronic document management systems are identified. It was concluded that when using modern electronic document management systems, the above described groups of methods and means of information protection should be used in combination. The basic requirements for electronic document management systems as a whole are considered, and additional requirements for secure electronic document management systems are defined. The architecture and the basic principles of constructing a system for the protection of EDS are analyzed. Information security is implemented using the example of the SMBusiness electronic document management system.

Degree of use: The obtained results were introduced into the educational process at the department of design of information and computer systems of the educational institution "Belarusian State University of Informatics and Radioelectronics" in the lecture course "Project management".

Sphere of application: institutions of higher education.