# ИНФОРМАТИКА И УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ И СОЦИАЛЬНЫХ СИСТЕМАХ

**УДК 004.65**

**Е.А. Грошева[2], И.В. Гусев[3], В.Н. Дмитриев[2], К.В. Ильичев[1], С.В. Куликов[2], С.А. Манцеров[1], А.Ю. Панов[1]**

## РАЗРАБОТКА ИНФОРМАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЯ, СООТВЕТСТВУЮЩИХ ФЕДЕРАЛЬНЫМ СТАНДАРТАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Нижегородский государственный технический университет им. Р.Е. Алексеева[1],
Научно-исследовательский институт измерительных систем им. Ю.Е. Седакова[2],
Российский федеральный ядерный центр Всероссийский
научно-исследовательский институт экспериментальной физики [3]

Рассматривается задача создания корпоративного портала предприятия, соответствующего федеральным стандартам обеспечения безопасности информации. Приводятся результаты анализа использования серверных операционных систем и офисного программного обеспечения в федеральных государственных информационных системах, а также результаты разработки автоматизированной информационной системы - рабочего программного обеспечения «Корпоративный портал». Предоставляется описание составляющих модулей и разработанного рабочего интерфейса информационного портала.

*Ключевые слова:* безопасность информации, информационная система предприятия, операционные системы, сертифицированное программное обеспечение, сертификация.

Жизнь современного предприятия невозможно представить без локальной вычислительной сети (ЛВС), позволяющей осуществлять взаимодействия сотрудников, обмениваться корпоративной почтой и пользоваться хранящейся на сервере информацией. В зависимости от специфики производственной деятельности доступ к такой информации может быть свободным или ограниченным, причем последнее - необходимость ограничения доступа к какой-то части информации - присутствует всегда.

Учитывая совокупность задач, возлагаемых на ЛВС предприятия, зачастую возникает необходимость упорядочить и структурировать работу сети, и самое очевидное решение этой проблемы - создание сайта с соответствующими разделами (новости, справочники, статьи, базы данных и т.п.). Задача сама по себе несложная, учитывая, что существует масса конструкторов сайтов, позволяющих даже не очень квалифицированному программисту создать сайт с минимально достаточным функционалом.

Однако программный код такого сайта, как правило, не исследуется на возможные уязвимости, особенно если ЛВС предприятия не имеет выхода в глобальную сеть. Априори предполагается, что враг снаружи, сотрудники лояльны и вероятность хакерских атак внутри сети низкая. Между тем, даже потенциальная возможность неких деструктивных действий может представлять серьезную угрозу для деятельности предприятия.

В Реестре федеральных государственных информационных систем, размещенном на сайте Роскомнадзора по состоянию на май 2016 г. числится 339 информационных систем, причем это системы государственных структур, таких как МВД, МИД, ФМБА, ФК России,

ГАС "Выборы", АИС "Юстиция"и др. [1]. Все они являются по сути порталами, имеющими выход в глобальную сеть и, соответственно, разработанными с учетом, в том числе, и требований безопасности информации.

Попробуем проанализировать, хотя бы в общих чертах, из чего складывается безопасность информации, обрабатываемой в некой информационной системе. Очевидно, как минимум два фактора серьезно влияют на этот аспект - операционная система (ОС), а также рабочее программное обеспечение (РПО), эту информацию обрабатывающее. Основываясь на данных, приведенных в Реестре ФГИС, распределение серверных операционных систем, используемых этими системами, мы получили следующее распределение, представленное на рис. 1.

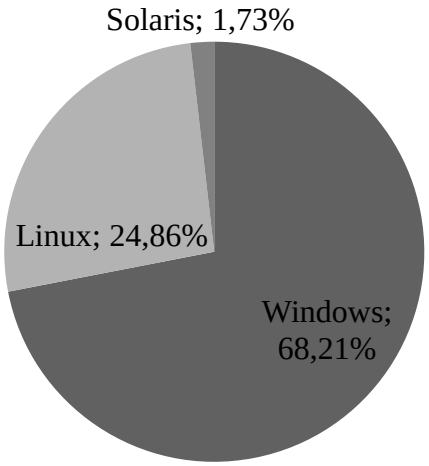


**Рис. 1. Процентное соотношение используемых серверных ОС**

Использование остальных ОС (FreeBSD, IBM-AIX, Unix, HP-UX, Novell NetWare, МСВС и Циркон) ничтожно мало.

При этом распределение по клиентским ОС, %:

- Windows - 70,41;
- Linux - 12,96%;
- MacOS - 10,37%.

Распределение функционирующих систем управления базами данных (СУБД) представлено на рис. 2.

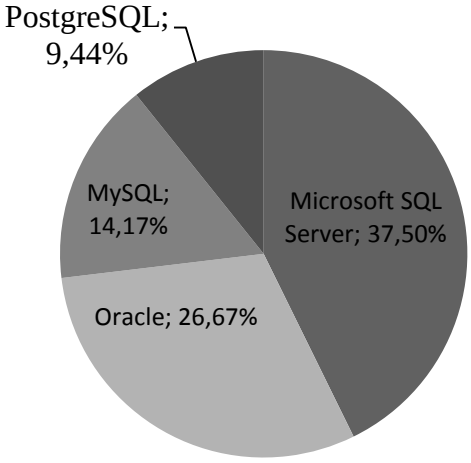


**Рис. 2. Процентное соотношение используемых СУБД**

Процентное соотношение использования офисного ПО представлено двумя платформами и соответственно составляет:

- Microsoft Office - 94,01%;
- Open\Libre Office - 5,99%.

Приведенная статистика показывает, что в подавляющем большинстве случаев даже в федеральных государственных информационных системах используются ОС семейства Windows. Говорить об их защищенности (за исключением отдельных релизов, имеющих соответствующие сертификаты) не приходится. Это проприетарное ПО с недоступным для анализа кодом[2].

Операционные системы на базе Linux можно разделить на два класса:

- ОС на базе ядра RedHat;
- ОС на базе ядра Debian.

Первый является коммерческим дистрибутивом (юрисдикция США), второй - некоммерческий дистрибутив внегосударственной юрисдикции.

На базе RedHat разработаны такие отечественные операционные системы, как ОС МСВС, ОС "Альт Линукс", ОС "Роса", ОС "Заря". Последние три ОС базируются на средствах защиты информации - SELinux, разработка Агентства национальной безопасности США.

На базе Debian есть единственная отечественная ОС - AstraLinux, разработки компании РусБИТех. Средства защиты информации, применяемые в ней (и в ОС МСВС) - отечественной разработки.

Вопросы необходимости импортозамещения в случае выбора ОС и рабочего программного обеспечения, используемого как в ФГИС, так и в порталах и сайтах менее крупных предприятий, учреждений и госструктур - это в первую очередь вопросы именно информационной безопасности этих систем. Но если с операционными системами, сертифицированными по требованиям безопасности информации, хоть какой-то выбор есть, то с РПО ситуация, как правило, сложнее. Проходить процедуру сертификации во ФСТЭК готовы далеко не все разработчики, так как она требует существенных временных и финансовых издержек и существенно осложняет процесс разработки. Учитывая, что к вопросам создания корпоративных порталов зачастую подходят из остаточных принципов, закладывать в этот процесс процедуру сертификации такого РПО готовы и не все заказчики.

Было разработано рабочее программное обеспечение РПО "Корпоративный портал" (Веб-портал предприятия), которое в мае 2016 г. получило сертификат соответствия требованиям безопасности информации ФСТЭК России. Данное РПО функционирует в среде операционной системы "AstraLinuxSpecialEdition" версии 1.3, является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации и соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999) - по уровню 2 контроля [2].

Данное РПО предназначено для организации совместной работы сотрудников предприятия и решает следующие задачи:

- создание логики «Одного окна». Портал позволяет собрать в одном месте все ключевые и часто используемые сотрудниками ресурсы и приложения. Достаточно открыть страницу в браузере – и все важные документы, необходимые контакты, назначенные задачи и последние новости окажутся перед глазами;
- внутренние коммуникации. Корпоративный портал дает широкие возможности для увеличения эффективности внутренних коммуникаций за счет встроенного модуля обмена мгновенными сообщениями;

- управление документами. Функционал корпоративного портала позволяет минимизировать ручные операции и максимально перейти на электронную форму документооборота за счет единого хранилища документов с поддержкой системы контроля версий;
- интеграция. Портал может быть интегрирован с рядом внутренних и внешних систем организации (например, почтовый клиент), что позволит эффективнее использовать все перечисленные системы;
- безопасность. Внутренний портал обеспечивает надежное хранение информации благодаря строгому, но гибкому разграничению прав доступа и ролей пользователей.

Функционал корпоративного портала позволяет оптимизировать работу всех жизненно важных областей работы организации.

В состав программы входят следующие модули:

- главной страницы;
- календаря;
- адресной книги;
- сообщений;
- корпоративного поиска;
- документов;
- новостей;
- управления проектами;
- базы знаний;
- совместного обучения.

Количество и содержание модулей зависит от настроек системы и определяется правами пользователя. Так, модуль «Администрирование» присутствует только у администраторов системы.

Также интерфейс системы зависит от прав пользователя, с которыми он вошел в систему. Так, при правах, отличных от НС (несекретно), интерфейс по созданию новостей/страниц базы знаний будет недоступен.

Слева на главной странице находится навигационная панель с ссылками на доступные пользователю модули и пиктограммы уведомлений о новых событиях. Центральный блок содержит ссылки и описания на последние новости, задания и события. Изображение главной страницы РПО "Корпоративный портал" приведено на рис. 3.

Модуль календаря позволяет пользователю создавать и получать уведомления о событиях, таких как личные напоминания, запланированные совещания по какому-либо проекту. Модуль Календарь предоставляет следующие возможности:

- планирование личных событий;
- отображение дней рождений сотрудников;
- планирование рабочих встреч и событий;
- оповещение других участников о событиях/встречах.


**Рис. 3. Главная страница РПО "Корпоративный портал"**

На главной странице модуля календарь пользователь может выбрать для отображения следующие фильтры:

- личные;
- дни рождения;
- рабочие.

Изображение страницы модуля календаря приведено на рис. 2.

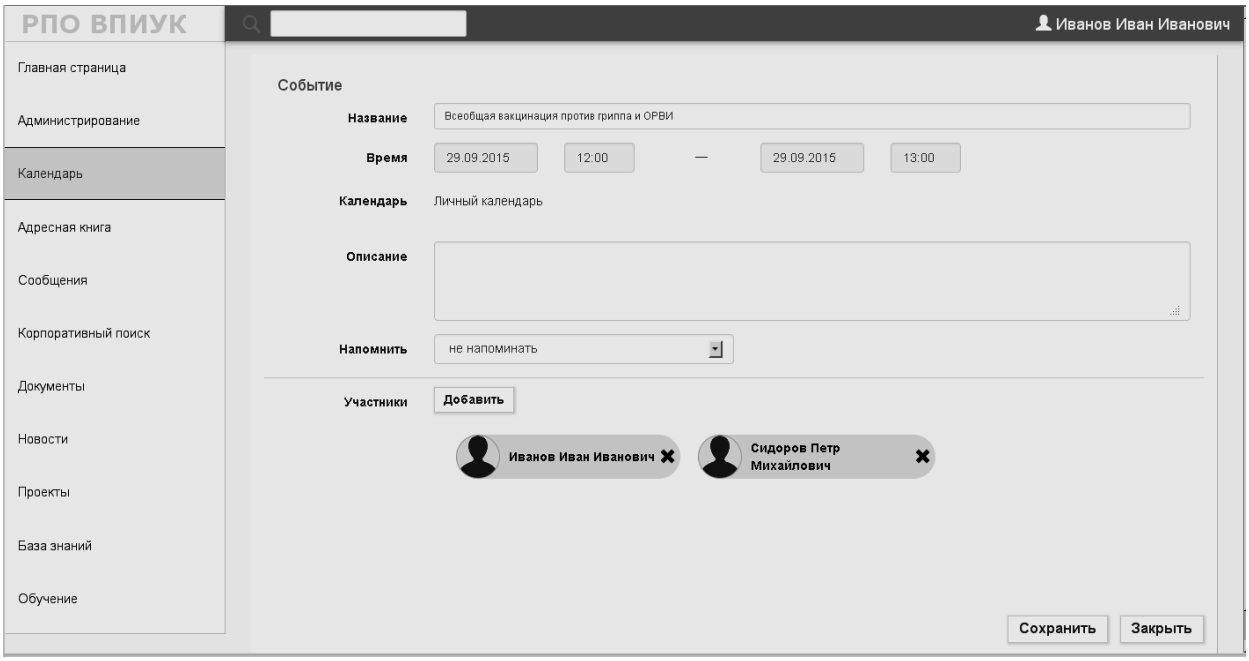


**Рис. 4. Страница модуля календаря РПО "Корпоративный портал"**

Записи личного календаря доступны только владельцу календаря по умолчанию. Данный тип создан для личных отметок, событий, напоминаний пользователя. Можно также добавить участников к событию. Тогда это событие будет видно всем участникам.

Записи дней рождений доступны всем пользователя ВПИУК и обновляются автоматически. Записи рабочего календаря содержат события/встречи, отражающие процесс выполнения проектов. Данные записи состоят из встреч/событий проектов, в которых пользователь является руководителем или исполнителем. Руководители проектов могут вносить коррективы в календарные записи или создавать дополнительные. После этого данные рабочего календаря всех участников проектов автоматически обновляются.

Модуль календарь имеет следующие виды отображения информации:

- день;
- месяц;
- год.

Модуль адресной книги построен на основе справочника сотрудников предприятия, сгруппированных по подразделениям. Содержит так же функцию поиска по заданным критериям. Также данный модуль предоставляет возможность  просмотра контактов. При этом профиль сотрудника может содержать следующие поля:

- фамилия;
- имя;
- отчество;
- дата рождения;
- предприятие, подразделение;
- должность;

- рабочий телефон;
- мобильный телефон;
- адрес электронной почты.

Изображение страницы модуля адресной книги приведено на рис. 5.

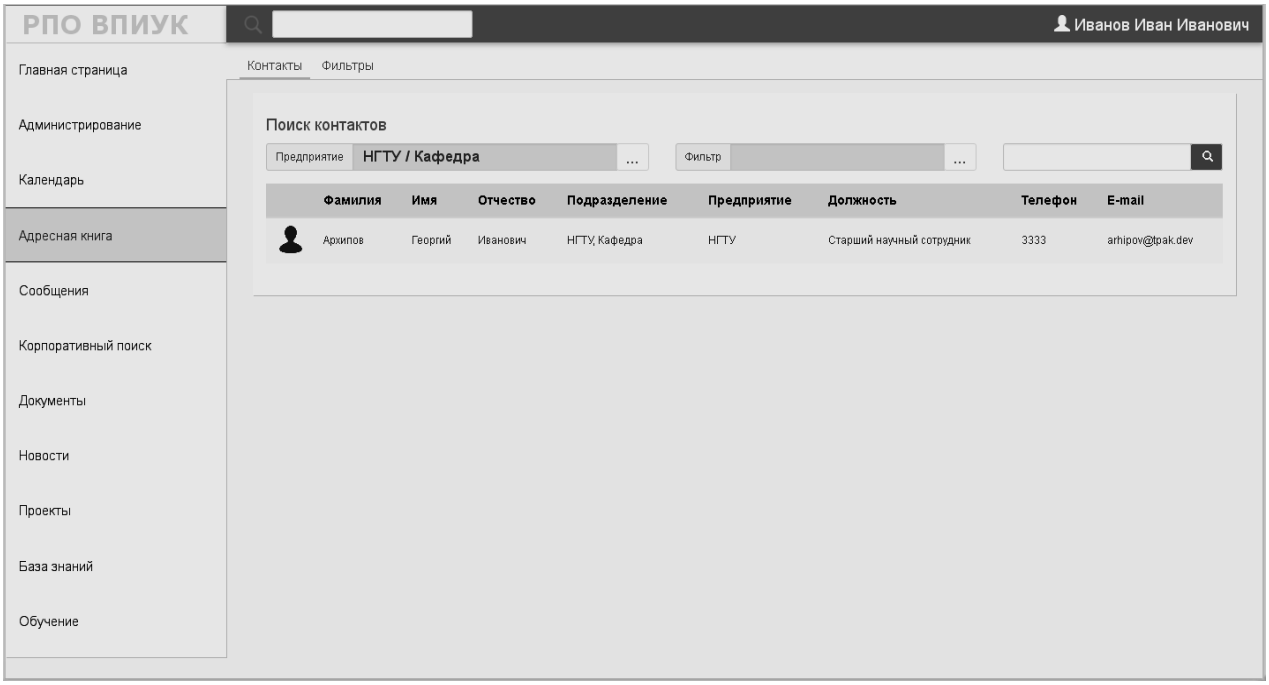


**Рис. 5. Страница модуля адресной книги РПО "Корпоративный портал"**

Модуль сообщений служит для обмена моментальными сообщениями между сотрудниками. При получении нового сообщения приходит соответствующее уведомление. Есть возможность настройки списка контактов.

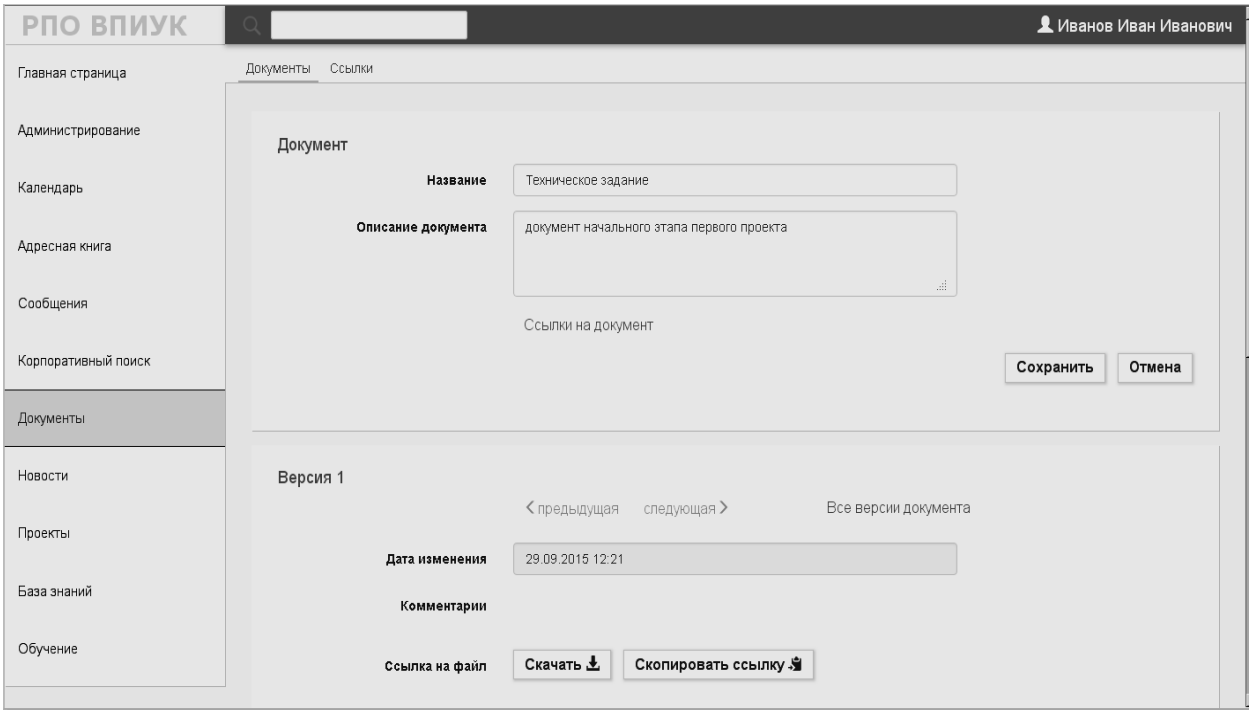


**Рис. 6. Страница модуля документов РПО "Корпоративный портал"**

Модуль документов построен на основе двух структур: структуры описывающей документ и его версии и структуры, описывающей права доступа пользователей по отношению к документу. Данный модуль обеспечивает создание и доступ к документам пользователя. В качестве документа может выступать файл любого типа. Каждое изменение документа приводит к увеличению версии документа (файла).

Изображение страницы модуля документов приведено на рис. 6.

Модуль новостей построен на основе списка новостных статей. Новостная лента может отображаться в режиме потока новостей, новостей по соответствующим тегам, а также в режиме Архив. Пользователь может создавать собственный пост, перейдя по ссылке «Добавить новость». В данном модуле также предусмотрен поиск.

Модуль базы знаний содержит справочные материалы и нормативные документы. В нем предусмотрены каталоги, включающие в себя информационные статьи. Существует возможность добавлять каталоги и статьи.

Модуль корпоративного поиска РПО ВПИУК позволяет осуществлять поиск информации по базам данных по заданным критериям, заданным в специальной поисковой строке. Результатом поиска является список контактов/документов, содержащий их названия и краткие аннотации, а также ссылки на страницы с полным описанием контакта/документа.

Модуль управления проектами позволяет пользователям совместно работать над документами, осуществлять планирование рабочих процессов, отслеживать ход работы над проектами.

Изображение страницы модуля управления проектами приведено на рис. 7.

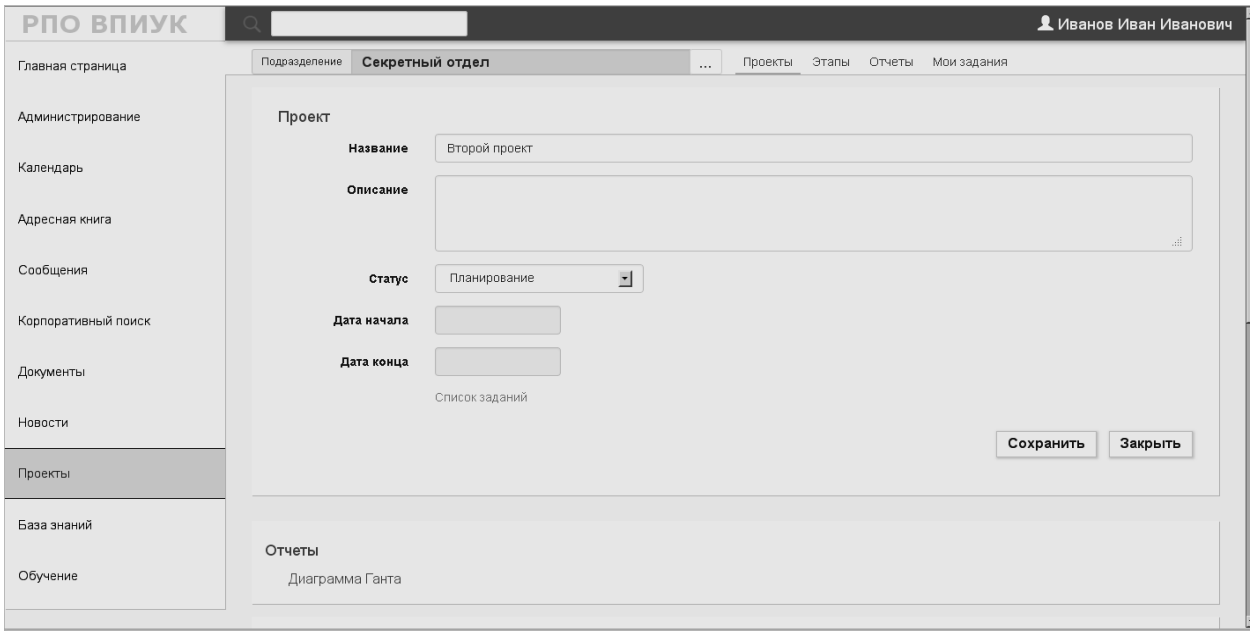


**Рис. 7. Страница модуля управления проектами РПО "Корпоративный портал"**

Модуль администрирования является базовым для настройки и администрирования данной информационной системы. В нем определяются права доступа пользователей и уровни конфиденциальности документов. В данном модуле возможны настройка приоритетов каждого сотрудника, редактирование профилей пользователей, выставление соответствующих прав доступа к различным модулям и каналам связи.

## Выводы

В настоящее время пренебрегать безопасностью информации, проходящей через программные платформы, неразумно. Бесспорно, полной безопасности в информационных системах достичь невозможно, однако применяя, а также рационально используя различные программные платформы, соответствующие сертификатам информационной безопасности можно существенно снизить вероятность реализации угрозы.

По результатам анализа серверных ОС, клиентских программных платформ, а также СУБД была проведена сегментация поля использования данных информационных продуктов, а также оценена их степень безопасности и защиты информационных данных.

Было разработано рабочее программное обеспечение РПО "Корпоративный портал", а также были проведены комплексные полигонные испытания данной информационной системы. В результате проведенной сертификации Федеральной службой по техническому и экспортному контролю было установлено полное соответствие РПО "Корпоративный портал", мерам информационной безопасности, предъявляемым к автоматизированным информационным системам класса 1Б.

**Библиографический список**


1. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [электронный ресурс]. - Режим доступа к ресурсу: http://www.rkn.gov.ru/.
2. **Савельев, А.И.** Лицензирование программного обеспечения в России: законодательство и практика / А. И. Савельев. – М.: Инфотропик Медиа, 2012. – 432 с. – ISBN 978-5-9998-0132-6.
3. Официальный сайт Федеральной службы по техническому и экспортному контролю [электронный ресурс]. - Режим доступа к ресурсу: http://fstec.ru/.
4. **Манцеров, С.А.** Мониторинг состояния объектов на основе методов функциональной систематики // Труды НГТУ им. Р.Е. Алексеева “Современные проблемы механики и автоматизации в машиностроении и на транспорте”, Н.Новгород, 2008. Т. 67.
5. **Манцеров, С.А.** Создание баз данных объектов машиностроения на основе формул функциональной систематики Вестник ВГТУ. 2007. Т. 3. №11.
6. **Манцеров, С.А.** Развитие систем единой функциональной систематики для хранения данных о техническом состоянии объекта / С.А. Манцеров, А.Ю. Панов // Вестник Нижегородского университета им. Н.И. Лобачевского. – Н. Новгород, 2013. – № 6 (ч. 1).


*Дата поступления*
*в редакцию 27.09.2016*

**E.A. Grosheva[2], I. V. Gusev[3], V.N. Dmitriev[2], K.V. Ilichev[1], S.V. Kulikov[2], S.A. Mancerov[1], A.Y. Panov[1]**

## DEVELOPMENT OF ENTERPRISE INFORMATION SYSTEMS, CORRESPONDING FEDERAL INFORMATION SECURITY STANDARDS

Nizhny Novgorod state technical university n.a. R.E. Alexeyev[1],
Scientific research institute of measuring systems n. a. Y.E. Sedakov[2],
Russian federal nuclear center All-Russian research institute of experimental Physics[3]

**Purpose:** Creation of a corporate enterprise portal, corresponding federal information security standards.
**Design/methodology/approach:** A theoretical framework is proposed based on methodology certification information systems and database management systems.
**Findings:** The results can be applied to the design and certification software platforms with a high level of protection of information.
**Research limitations/implications:** The present study provides the results of the analysis of the use of server operating systems and office software in the federal government information systems.
**Originality/value:** Viewed functionality, as well as the area to be solved by this developed an information platform, its objectives and specific certification, a detailed description of the structural components of the platform modules, as well as information portal designed operator interface can be used in the construction of complex enterprise information systems.

*Key words:* Information security, enterprise information system, operating systems, certified software, certification.