

УДК 004.65

**Е.А. Грошева<sup>2</sup>, И.В. Гусев<sup>3</sup>, В.Н. Дмитриев<sup>2</sup>, К.В. Ильичев<sup>1</sup>,  
С.В. Куликов<sup>2</sup>, С.А. Манцеров<sup>1</sup>, А.Ю. Панов<sup>1</sup>**

<sup>1</sup>Нижегородский государственный технический университет им. Р.Е. Алексеева

<sup>2</sup>Научно-исследовательский институт измерительных систем им. Ю.Е. Седакова

<sup>3</sup>Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики

## **РАЗРАБОТКА ЗАЩИЩЕННОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ**

В настоящее время, характеризующееся жесткой конкуренцией, а также динамическим состоянием рынка, большое количество предприятий испытывает потребность в автоматизации. Даже самые консервативные и небогатые компании ощущают выгоду от использования компьютерных технологий. При этом за довольно небольшой период времени программное обеспечение претерпело колоссальные изменения, пройдя путь от простейших арифметических программ до комплексных информационных систем, функционирующих на больших предприятиях. Применение подобных современных информационных технологий позволяет качественно улучшить производственные показатели. Однако параллельно с этим остро возникает вопрос обеспечения защиты информации. С непрерывным процессом проникновения во все общественные сферы средств обработки и передачи данных задача обеспечения информационной безопасности так же постоянно обостряется. При этом любое предприятие имеет достаточно информации, рассматриваемой с точки зрения необходимости ее защиты. Следует отметить, что данная проблема является многоплановой и комплексной, охватывающей ряд определенно важных задач.

В статье 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 со встроенными средствами защиты от несанкционированного доступа к информации – рабочего программного обеспечения «Корпоративный портал». Рассматриваются функционал, а также область решаемых данной разработанной информационной платформой задач и специфика ее сертификации. Предоставляется подробное описание структурных составляющих платформы модулей, а также разработанного рабочего интерфейса информационного портала.

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

**E.A. Grosheva<sup>2</sup>, I.V. Gusev<sup>3</sup>, V.N. Dmitriev<sup>2</sup>, K.V. Ilichev<sup>1</sup>,  
S.V. Kulikov<sup>2</sup>, S.A. Mancero<sup>1</sup>, A.Yu. Panov<sup>1</sup>**

<sup>1</sup>Nizhny Novgorod state technical university n. a. R.E. Alexeev

<sup>2</sup>Scientific research institute of measuring systems n. a. Yu.E Sedakov

<sup>3</sup>Russian federal nuclear center All-Russian research institute  
of experimental Physics

## **DEVELOPMENT OF AN AUTOMATED SECURE ENTERPRISE INFORMATION SYSTEM**

At the present time, characterized by strong competition and a dynamic market conditions, a large number of enterprises are in need of automation. Even the most conservative and rather poor company feel the benefit from the use of computer technology. At the same time in a relatively short period of time the software has undergone tremendous changes, starting as a simple arithmetic programs, to integrated information systems that operate on large enterprises. The use of these modern information technologies allows qualitatively improve the production performance. However, in parallel with this sharply raises the question of information security. With the continuous process of penetration into all spheres of public funds and the processing of data, the problem of information security as constantly escalates. At the same time any company has sufficient information, considered from the standpoint of the need to protect it. It should be noted that this problem is multifaceted and complex, encompassing a number of particularly important tasks.

The article deals with the problem of creating a corporate enterprise portal, the corresponding federal information security standards. The results of the analysis of the use of server operating systems and office software in the federal government information systems and the development of an automated information system with a built-in protection against unauthorized access to the information - operating software "Enterprise Portal". We consider the functional and domain solved this developed an information platform, tasks and specifics of its certification. It provides a detailed description of the structural components of the platform modules, and developed a working interface information portal.

**Keywords:** Information security, enterprise information system, operating systems, business software, certification.

**Введение.** 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 не сложная, 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.

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.

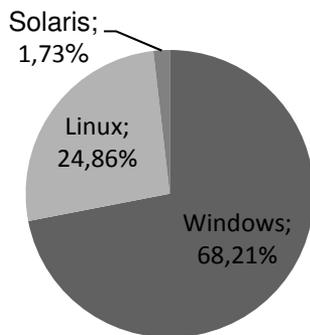


Рис. 1. Процентное соотношение используемых серверных ОС

Использование других ОС, таких как FreeBSD, IBM-AIX, Unix, HP-UX, Novell NetWare, MCBS и Циркон, ничтожно мало. При этом распределение по клиентским ОС следующее:

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

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

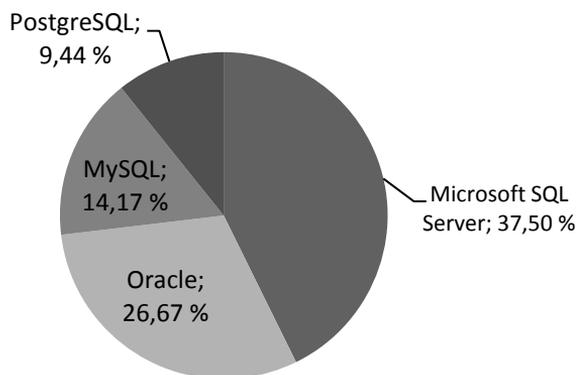


Рис. 2. Процентное соотношение используемых СУБД

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 [1].

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 – SE Linux, разработка Агентства национальной безопасности США.

На базе Debian есть единственная отечественная ОС – «Astra Linux», разработки фирмы «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 не все заказчики.

В Реестре федеральных государственных информационных систем, размещенном на сайте Роскомнадзора, по состоянию на май 2016 г. числятся 339 информационных систем, причем это системы государственных структур, таких как МВД, МИД, ФМБА, ФК России, ГАС «Выборы», АИС «Юстиция» и др. [2]. Все они являются, по сути, порталами, имеющими выход в глобальную сеть и, соответственно, разработанными, кроме прочего, с учетом требований безопасности информации.

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 Astra Linux Special Edition 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 недеklarированных возможностей» (Гостехкомиссия России, 1999) – по уровню 2-го контроля [3].

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

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.

Рассмотрим структуру разработанного информационного портала. В состав программы входят следующие модули:

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

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

Также интерфейс системы зависит от прав пользователя, с которыми он вошел в систему. Так, например, при правах, отличных от НС

(не секретно), 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.



Рис. 3. Главная страница РПО «Корпоративный портал»

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.

На главной странице модуля «Календарь» пользователь может выбрать для отображения следующие фильтры: личные; дни рождения; рабочие. 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. Изображение страницы модуля календаря приведено на рис. 4.

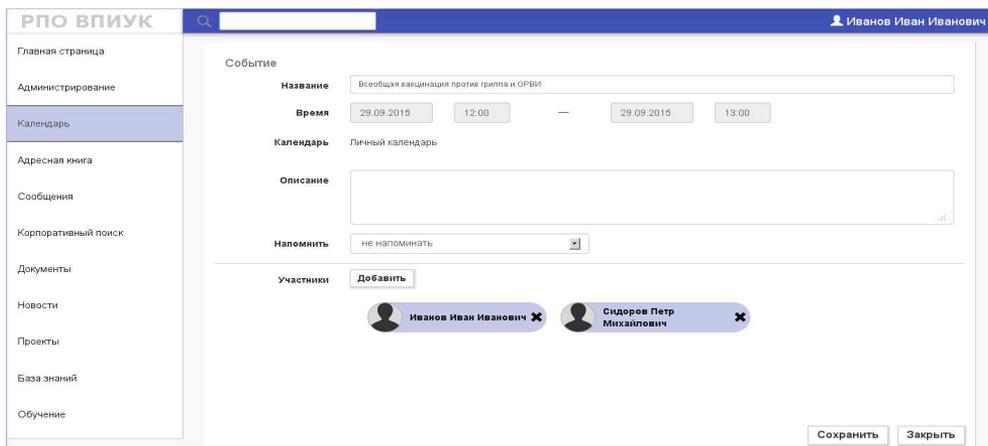


Рис. 4. Страница модуля календаря РПО «Корпоративный портал»

Записи дней рождений доступны всем пользователям 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 также функцию поиска по заданным критериям. К тому же 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.

Модуль сообщений служит для обмена моментальными сообщениями между сотрудниками. При получении нового сообщения приходит соответствующее уведомление. Есть возможность настройки списка контактов. Изображение страницы модуля сообщений приведено на рис. 6.

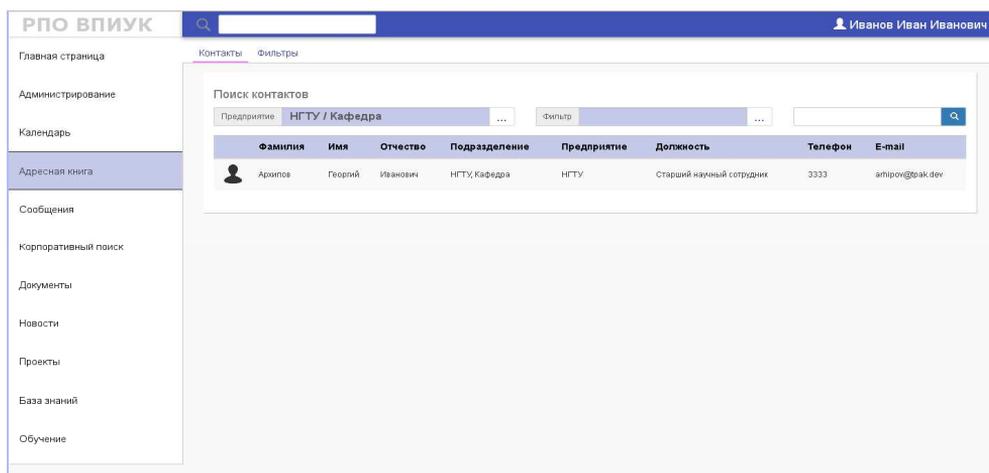


Рис. 5. Страница модуля адресной книги РПО «Корпоративный портал»

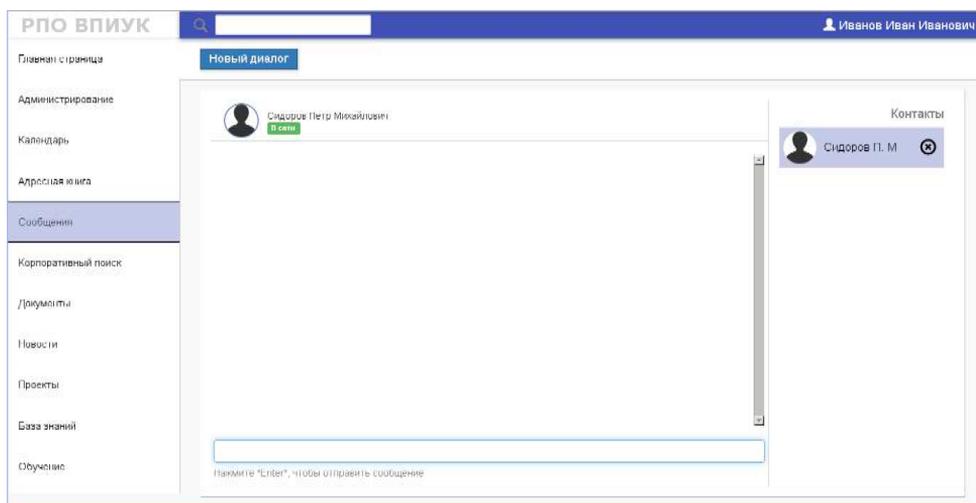


Рис. 6. Страница модуля сообщений РПО «Корпоративный портал»

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. 7.

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». Пользова-

тель может создавать собственный пост, перейдя по ссылке «Добавить новость». В данном модуле также предусмотрен поиск. Изображение страницы модуля новостей приведено на рис. 8.

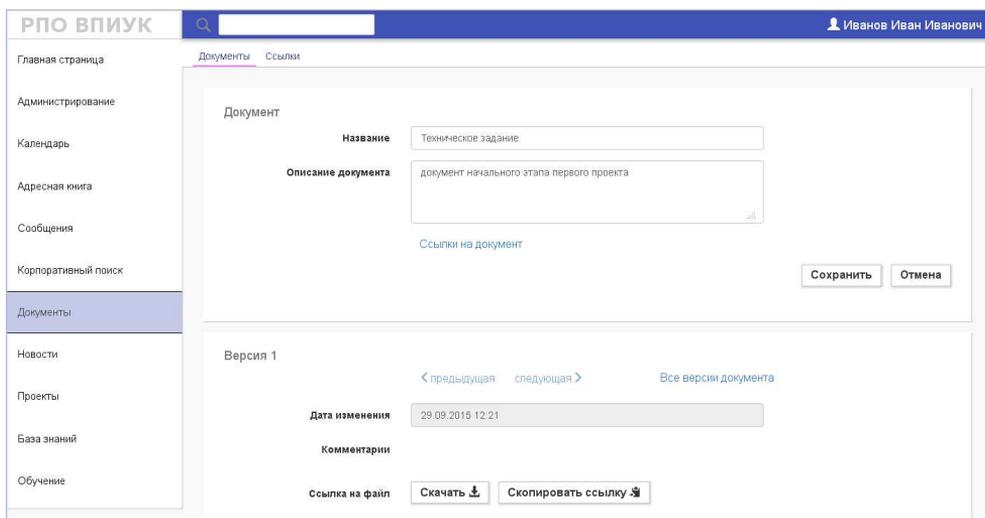


Рис. 7. Страница модуля документов РПО «Корпоративный портал»

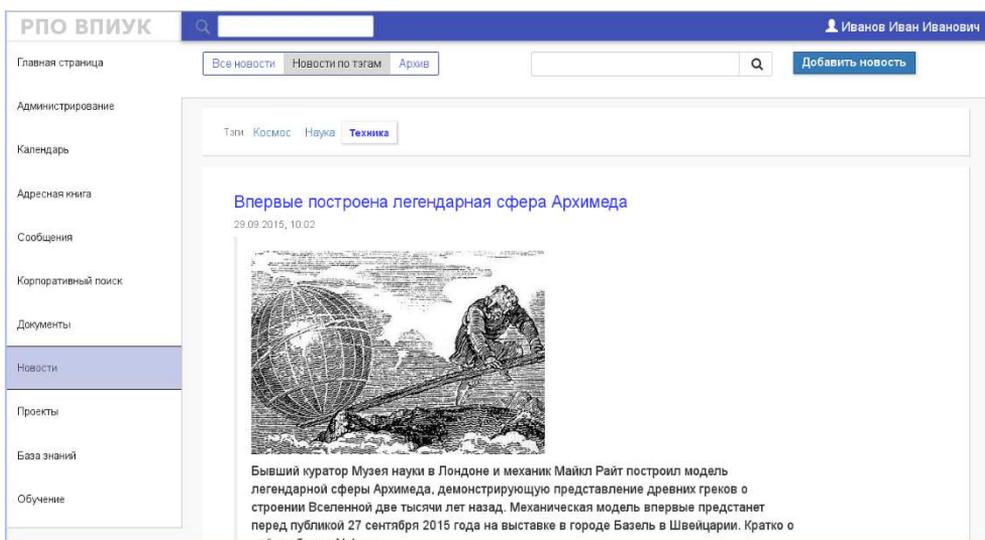


Рис. 8. Страница модуля новостей РПО «Корпоративный портал»

Модуль базы знаний содержит справочные материалы и нормативные документы. В нем предусмотрены каталоги, включающие в себя информационные статьи. Существует возможность добавлять каталоги и статьи. Изображение страницы модуля базы знаний приведено на рис. 9.

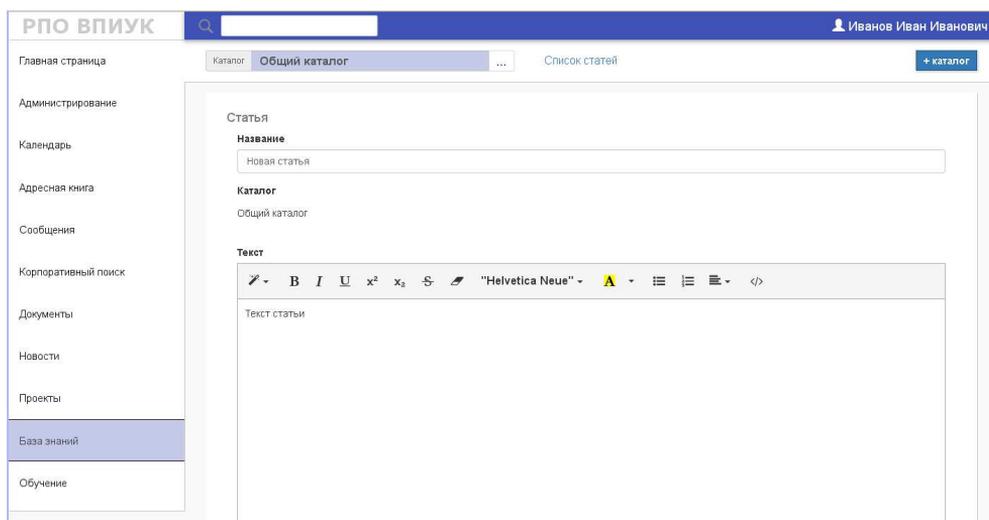


Рис. 9. Страница модуля базы знаний РПО «Корпоративный портал»

Модуль корпоративного поиска РПО ВПИУК позволяет осуществлять поиск информации по базам данных по заданным критериям, указанным 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. Изображенные страницы модуля управления проектами приведено на рис. 10.

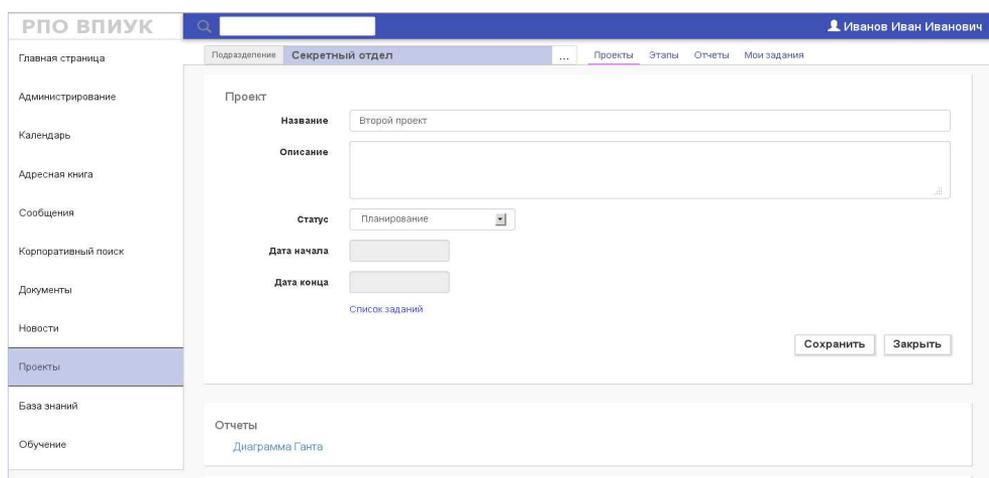


Рис. 10. Страница модуля управления проектами РПО «Корпоративный портал»

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. Изображение страницы модуля управления проектами приведено на рис. 11.

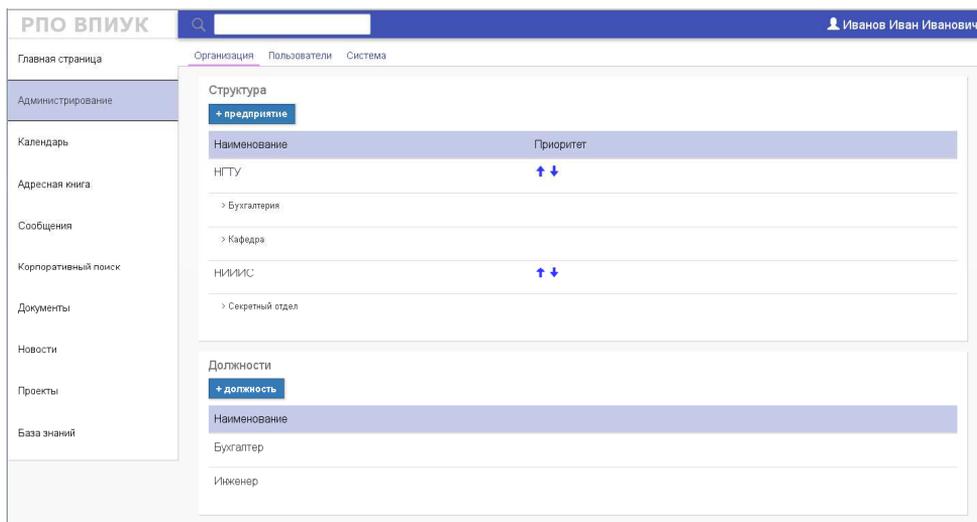


Рис. 11. Страница модуля администрирования РПО «Корпоративный портал»

**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 проведенного 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. Савельев А.И. Лицензирование программного обеспечения в России: законодательство и практика. – М.: Инфотропик Медиа, 2012. – 432 с.

2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]. – URL: <http://www.rkn.gov.ru> (дата обращения: 30.06.2016).

3. Официальный сайт Федеральной службы по техническому и экспортному контролю [Электронный ресурс]. – URL: <http://fstec.ru> (дата обращения: 30.06.2016).

4. Манцеров С.А. Мониторинг состояния объектов на основе методов функциональной систематики // Современные проблемы механики и автоматизации в машиностроении и на транспорте: тр. НГТУ им. Р.Е. Алексеева. – Н. Новгород, 2008. – Т. 67.

5. Манцеров С.А. Создание баз данных объектов машиностроения на основе формул функциональной систематики // Вестник Воронеж. гос. техн. ун-та. – 2007. – Т. 3. – № 11.

6. Манцеров С.А., Панов А.Ю. Развитие систем единой функциональной систематики для хранения данных о техническом состоянии объекта // Вестник Нижегород. ун-та им. Н.И. Лобачевского. – Н. Новгород, 2013. – № 6, ч. 1.

7. Васильев Р.Б., Калянов Г.Н., Лёвочкина Г.А. Управление развитием информационных систем. – М.: Горячая линия-Телеком, 2009. – 368 с.

8. Бородакий Ю.В., Лободинский Ю.Г. Эволюция информационных систем (современное состояние и перспективы). – М.: Горячая линия-Телеком, 2011. – 368 с.

9. Защита информации в компьютерных сетях. Практический курс: учеб. пособие // А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский [и др.]; под ред. Н.И. Синадского. – Екатеринбург: Изд-во УГТУ-УПИ, 2008. – 248 с.

10. Курбатов Д. Популярное сетевое оборудование и статистика уязвимостей / Positive Research, 2012. – URL: <https://habrahabr.ru/company/pt/blog/142479> (дата обращения: 30.06.2016).

## References

1. Savell'ev A.I. Litsenzirovaniie programmnoho obespecheniia v Rossii: zakonodatel'stvo i praktika [Software licensing in Russia: legislation and experience]. Moscow: Infotropik Media, 2012. 432 p.

2. Ofitsial'nyi sait Federal'noi sluzhby po nadzoru v sfere sviazi, informatsionnykh tekhnologii i massovykh kommunikatsii [Official web-site of Federal Service for Supervision of Communications, Information Technology and Mass Media], available at: <http://www.rkn.gov.ru> (accessed 30 June 2016).

3. Ofitsial'nyi sait Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontroliu [Official web-site of Federal Service for Technology and Export Control], available at: <http://fstec.ru> (accessed 30 June 2016).

4. Mantserov S.A. Monitoring sostoianiiia ob"ektov na osnove metodov funktsional'noi sistematiki [Monitoring the status of objects on the basis of methods of functional taxonomy]. *Trudy Nizhegorodskogo gosudarstvennogo tekhnicheskogo universiteta imeni R.E. Alekseeva "Sovremennye problemy mekhaniki i avtomatizatsii v mashinostroenii i na transporte"*, 2008, vol. 67.

5. Mantserov S.A. Sozdanie baz dannykh ob"ektov mashinostroeniiia na osnove formul funktsional'noi sistematiki [Designing databases of the machinery objects according to functional taxonomy formula]. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta*, 2007, vol. 3, no. 11.

6. Mantserov S.A., Panov A.Iu. Razvitie sistem edinoi funktsional'noi sistematiki dlia khraneniia dannykh o tekhnicheskome sostoianii ob"ekta [The single functional taxonomy system development for storing data, devoted to technical characteristic of the object]. *Vestnik Nizhegorodskogo universiteta imeni N.I. Lobachevskogo*, 2013, no. 6, part 1.

7. Vasil'ev R.B., Kalianov G.N., Levochkina G.A. Upravlenie razvitiem informatsionnykh sistem [Management of information system development]. Moscow: Goriachaia liniia-Telekom, 2009. 368 p.

8. Borodakii Iu.V., Lobodinskii Iu.G. Evoliutsiia informatsionnykh sistem (sovremennoe sostoianie i perspektivy) [Information system evolution (state-of-the-art and strategy)]. Moscow: Goriachaia liniia-Telekom, 2011. 368 p.

9. Andronchik A.N., Bogdanov V.V., Domukhovskii N.A. [et al.]. Zashchita informatsii v komp'iuternykh setiakh. Prakticheskii kurs [Information security in computer networks. Apprentice course]. Ekaterinburg: Ural'skii gosudarstvennyi tekhnicheskii universitet – UPI imeni pervogo Prezidenta Rossii B.N. El'tsina, 2008. 248 p.

10. Kurbatov D. Populiarnoe setevoe oborudovanie i statistika uiazvimostei [Popular network hardware and holes statistics]. Positive Research, 2012, available at: <https://habrahabr.ru/company/pt/blog/142479> (accessed 30 June 2016).

### **Сведения об авторах**

**Грошева Екатерина Альбертовна** (Н. Новгород, Россия) – ведущий инженер-исследователь Научной исследовательской группы 3102 Научно-исследовательского института измерительных систем им. Ю.Е. Седакова (603137, Н. Новгород, ул. Тропинина, 47, тел.: 8 (831) 469-57-09).

**Гусев Игорь Владимирович** (Саров, Россия) – заместитель главного конструктора Российского федерального ядерного центра Всероссийского научно-исследовательского института экспериментальной физики (607188, Нижегородская обл., г. Саров, пр. Музрукова, 10, тел.: 8 (83130) 2-78-73).

**Дмитриев Владимир Николаевич** (Н. Новгород, Россия) – ведущий специалист Научной исследовательской группы 3102 Научно-исследовательского института измерительных систем им. Ю.Е. Седакова (603137, Н. Новгород ул. Тропинина, 47, тел.: 8 (831) 469-57-09).

**Ильичев Кирилл Владимирович** (Н. Новгород, Россия) – магистрант Нижегородского государственного технического университета им. Р.Е. Алексеева, Института промышленных технологий машиностроения кафедры автоматизации машиностроения (603155, Н. Новгород, ул. Минина, д. 26, корп. 4, ауд. 4210, тел.: 8-908-739-70-08, e-mail: kirill989ilichev@gmail.com).

**Куликов Сергей Валентинович** (Н. Новгород, Россия) – заместитель главного конструктора, начальник Департамента развития автоматизированных систем управления и вычислительных устройств Научно-исследовательского института измерительных систем им. Ю.Е. Седакова (603137, Н. Новгород, ул. Тропинина, 47, тел.: 8 (831) 466-16-03).

**Манцеров Сергей Александрович** (Н. Новгород, Россия) – заведующий кафедрой автоматизация машиностроения Института промышленных технологий машиностроения Нижегородского государственного технического университета им. Р.Е. Алексеева, кандидат технических наук, доцент (603155, Н. Новгород, ул. Минина, д. 26, корп. 4, ауд. 4202, тел.: 8 (831) 436-73-54, e-mail: sergei639@gmail.com).

**Панов Алексей Юрьевич** – директор Института промышленных технологий машиностроения Нижегородского государственного тех-

нического университета им. Р.Е. Алексева, заведующий кафедрой теоретической и прикладной механики, доктор технических наук, профессор (603155, Н. Новгород, ул. Минина, д. 26, корп. 4, ауд. 4210, тел.: 8 (831) 436-80-85, e-mail: fam@nntu.nnov.ru).

### **About the authors**

**Grosheva Ekaterina Albertovna** (Nizhny Novgorod, Russian Federation) leading Research Engineer Scientific Research Group 3102 "Scientific Research Institute of Measuring Systems of Yu.E. Sedakov" (603137, N. Novgorod, Tropinina str. 47, tel.: 8 (831) 469-57-09).

**Gusev Igor Vladimirovich** deputy chief designer of "Russian Federal Nuclear Center, All-Russian Research Institute of Experimental Physics" (607188, Sarov, pr. Muzrukova 10, tel.: 8 (83130) 2-78-73).

**Dmitriev Vladimir Nikolaevich** (Nizhny Novgorod, Russian Federation) leading Specialist of the Scientific Research Group 3102 "Scientific Research Institute of Measuring Systems of Yu.E. Sedakov" (603137, N. Novgorod, Tropinina str. 47, tel.: 8 (831) 469-57-09).

**Ilichev Kirill Vladimirovich** (Nizhny Novgorod, Russian Federation) 1st year student of Magistracy Institute of Industrial Engineering Technology, of the department "Automation Engineering" Russia, (603000, N. Novgorod, Zvezdinka 26A, tel.: 8-908-739-70-08, e-mail: kirill989ilichev@gmail.com).

**Kulikov Sergej Valentinovich** (Nizhny Novgorod, Russian Federation) deputy Chief Designer, Head of Department of automated control systems and computing devices, "Scientific Research Institute of Measuring Systems of Yu.E. Sedakov" (603137, N. Novgorod, Tropinina str. 47, tel.: 8 (831) 466-16-03).

**Mantserov Sergey Aleksandrovich** (Nizhny Novgorod, Russian Federation) head of the department "Automation Engineering", Institute of industrial engineering technology named the Nizhny Novgorod state technical university, R.E. Alekseeva, docent (603155, N. Novgorod, Minina str. 26, aud. 4202, tel.: 8 (831) 436-73-54), e-mail: sergei639@gmail.com).

**Panov Aleksej Yurevich** (Nizhny Novgorod, Russian Federation) director of the Institute of Industrial Technologies Engineering named the Nizhny Novgorod state technical university, R.E. Alekseeva, head of chair "Theoretical and Applied Mechanics", Doctor of Technical Sciences, Professor (603155, N. Novgorod, Minina str. 26, aud. 4210, tel.: 8 (831) 436-80-85, e-mail: fam@nntu.nnov.ru).

Получено 12.10.2016