Обеспечение безопасности при цифровизации учебных заведений*

Г. П. Акимова, А. Ю. Даниленко, Е. В. Пашкина, М. А. Пашкин,
А. А. Подрабинович, А. В. Соловьев, И.В. Туманова

Федеральное государственное учреждение "Федеральный исследовательский центр "Информатика и управление" Российской академии наук", г. Москва, Россия

Аннотация. В статье рассмотрены особенности работы высших учебных заведений, включая деловые процессы в этих структурах. Сделан вывод о необходимости цифровизации не отдельных направлений работы, а всей деятельности института или университета, обоснована целесообразность решения этой задачи с помощью внедрения единой информационной системы, которая объединит все используемые в настоящее время и перспективные автоматизированные информационные системы. Рассмотрены вопросы обеспечения информационной безопасности при реализации этого решения.

Ключевые слова: высшее учебное заведение, информационная безопасность, деловые процессы организации, цифровизация, автоматизированные информационные системы.

DOI 10.14357/207186321904010

Введение

Работы по автоматизации работы институтов и университетов были начаты в нашей стране в 1970-е годы. Так, силами НИИ высшей школы СССР был создан комплекс программ, известный под названием «АСУ ВУЗ». Данный комплекс централизованно внедрялся в крупнейшие ВУЗы страны, имеющие наибольший технический и интеллектуальный потенциал, всего охвачено проектом было более 50 учебных заведений [1]. Разработка аналогичных систем в наше время активно ведется многими коллективами: коммерческими фирмами [2], самими учебными заведениями, государственными организациями. Так, в стадии разработки находится автоматизированная система управления высшим учебным заведением [3], а среди внедренных и успешно работающих систем отметим [4, 5]. Значительное число работ посвящено обзорам и осмыслению накопленного опыта в части автоматизации различных участков работы учебных заведений, например [6]. Эта тема включается в учебные курсы различных учебных заведений, ведущих подготовку по направлениям, посвященным разработке автоматизированных систем управления (АСУ) различного назначения [7].

В настоящее время автоматизация деловых процессов высших учебных заведений, включая научную составляющую их деятельности, выходит на новый этап, когда затрагиваются не только основные виды деятельности, но и вся жизнь институтов и университетов. При решении этой задачи возникает целый ряд вопросов, касающихся не только проектирования, но и разработки,

*Работа выполнена при частичной финансовой поддержке РФФИ в рамках научного проекта № 17-29-03263

внедрения вычислительных комплексов, реализующих требуемый функционал. Работа [8] посвящена цифровизации научно-исследовательских организаций, в том числе, обеспечению информационной безопасности. В данной статье авторы рассматривают аналогичные проблемы для ситуации учебного заведения.

Научные подразделения, как в составе научно-исследовательской организации, так и в учебном учреждении, относятся к коллективам, работа которых автоматизируется наиболее сложно в силу специфики. При этом речь идет не об экспериментальных работах, т.к. эта сфера деятельности автоматизируется программным обеспечением, входящим в состав применяемого экспериментального оборудования, а о творческой деятельности: изучении внешних источников информации, подготовки научных статей и отчетов, общении с коллегами из других институтов и государств, участие в Скайп - конференциях и вебинарах. Однако не следует забывать и о таких повседневных действиях, как фиксация рабочего времени, подготовка различных служебных записок и заявлений и пр. Для учебного заведения к упомянутым особенностям добавляются учет посещаемости студентов и преподавателей, формирование расписания занятий с учетом наличия аудиторий, проведение экзаменов и зачетов, проведение вступительных экзаменов и т.д.

Сложность автоматизации в данном случае связана с такими особенностями деловых процессов, как: работа с информацией различного уровня конфиденциальности, в том числе, с персональными данными преподавателей, студентов и сотрудников, а также с секретными данными при проведении научно-исследовательских работ; большое число участвующих сотрудников и студентов; использование различных прикладных программ, в том числе текстовых процессоров; программ для подготовки презентаций и различных иллюстраций; активное использование Интернет.

1. Особенности работы научных и учебных подразделений

Выделим основные деловые процессы, которые полностью или частично могут подлежать автоматизации в институте или университете.

1. Работа институтских кафедр и деканатов, включая составление расписаний занятий, консультаций, зачетов, экзаменов. В данном случае также необходимо отметить подготовку и проведение различных заседаний и совещаний, учет посещаемости студентов и преподавателей, сбор и хранение различных документов с организацией их каталога для быстрого поиска.

2. Учебно-методическая работа, в том числе подготовка и обсуждение учебных программ, курсовых и дипломных работ.

3. Работа учебных и научных лабораторий. В этот деловой процесс, подлежащий автоматизации, входят ведение журналов инструктажа по технике безопасности, подготовка инструкций, формирование заявок на закупку расходных материалов, а также лабораторного оборудования.

4. Материально-техническое обеспечение учебной работы.

5. Управление экспериментами. Деловой процесс включает в себя планирование эксперимента, его проведение, сбор и обработку результатов с последующим их обобщением, визуализацией и хранением полученных данных.

6. Организация студенческого обмена, в том числе с зарубежными институтами и университетами.

7. Работа ученого совета университета или института. В данном случае требуется учесть как планирование работы совета, так и сбор необходимых информационных материалов. Возможна частичная автоматизация действий, выполняемых в процессе заседания, а также контроля исполнения решений. Отдельной задачей является архивное хранение таких материалов, как протоколы заседаний, решения и отчеты об их выполнении, видеозаписи заседаний.

8. Подготовка научно-образовательных мероприятий (семинаров, конференций, круглых столов и др.). Особенностью процесса является обязательное наличие этапа планирования мероприятия, включая сбор предложений и составление программ. Кроме того, процесс включает в себя рассылку приглашений и сбор заявок от участников, подготовку и рецензирование полученных материалов, в том числе текстов докладов, подготовку проектов решений и контроль их выполнения.

9. Редакционно-издательская деятельность, в том числе сбор и рецензирование статей для публикации в научных журналах, издаваемых учебным заведением, ведение базы данных рецензентов с возможностью их полуавтоматического подбора в соответствии с тематикой публикуемых материалов. Сюда же следует отнести издание учебных пособий, методичек, руководств по лабораторным работам.

10. Работа библиотеки. Этот деловой процесс подразумевает, по сути, создание электронной библиотечной системы, в которую входят поисковая и учетная системы, а также программы оформления библиографических карточек.

11. Деятельность государственных аттестационных комиссий и диссертационных советов. Для данного процесса могут быть автоматизированы такие операции, как прием документов, подбор оппонентов и групп экспертов по диссертации или выпускной квалификационной работе в соответствии с ее специализацией, публикация текста диссертации на сайте института или университета, а также отправка документов в ВАК. Отдельной задачей в этой части является подготовка решений совета и ведение его архива.

12. Работа отделов аспирантуры и докторантуры в части приема заявок и документов от поступающих, подготовки и проведении экзаменов, а также подготовки и хранения различных документов.

13. Деятельность научно-образовательных центров университетов. Деловой процесс может включать такие задачи, как составление и рассылка приглашений преподавателям, автоматизация проведения тематических курсов лекций, подготовка необходимых документов, контроль успеваемости и др.

14. Экспертная оценка научных проектов: прием заявок на экспертизу, ведение базы данных экспертов и их подбор в соответствии с тематикой проекта, обработка заключений экспертов и оценка качества их работы.

15. Подбор персонала. Специфика данного делового процесса заключается в том, что институтские преподаватели – это уникальные кадры. Типовые кадровые агентства и службы могут не выявить специалистов нужной квалификации, т.к. обычно не обладают соответствующими компетенциями. При оценке кандидатур необходимо проводить анализ данных о кандидате с учетом требований к нему, включая автоматизированный анализ результатов научной и преподавательской деятельности. Подсистема автоматизации подбора персонала может быть дополнением к кадровой системе института.

16. Другие виды деятельности. К таким видам можно отнести ведение договоров с внешними партнерами, а также документооборот и делопроизводство.

2. Предлагаемый подход к автоматизации учебных заведений

Как видно из [1–7], основное направление работ при автоматизации учебных заведений состоит в разработке новой системы, состоящей из большого числа подсистем, каждая из которых предназначена для автоматизации одного определенного участка работы: работа с абитуриентами, планирование учебной работы со студентами, контроль и учет учебной работы, семейство кадровых подсистем, материально-техническое обеспечение и т.д. Этот подход имеет право на существование, но он полностью игнорирует то обстоятельство, что сейчас, в отличие от второй трети прошлого века, в любом институте или университете используется огромное количество автоматизированных систем, разработанных различными группами программистов. Эти системы, зачастую, никак между собой не связаны, организовать взаимодействие между ними крайне затруднительно, а порой и невозможно.

Для решения задачи полной автоматизации учебного заведения необходимо создание информационной системы нового типа (комплексная система управления, КСУ), которая объединит все работающие в настоящее время, а также перспективные, информационные и автоматизированные системы в единый программный комплекс. Это потребует доработки имеющихся систем для организации совместной работы только с одной объединяющей информационной системой, а не со всеми используемыми в настоящее время.

КСУ обеспечит и решение задачи передачи разнородной информации между пользователями и другими АИС, причем уже в процессе разработки в нее целесообразно включить подсистемы, обеспечивающие гарантированную доставку информации, протоколирование всех существенных действий и событий, контроль подлинности пользователей и системных процессов, а также аутентичности обрабатываемых документов. При этом необходимо отметить, что внедрение КСУ возможно только в случае решения целого ряда задач, связанных с обеспечением информационной безопасности.

3. Особенности применения средств защиты информации

3. 1. Информационные объекты

При разработке и внедрении КСУ потребуется формализовать понятие информационного объекта с целью обеспечения работы системы с информацией всех подключенных к ней внешних систем. Тем самым необходимо сформулировать требования к информационным объектам КСУ:

– объект создается, редактируется и уничтожается прикладной АИС, но при этом ряд его свойств обрабатывается КСУ;

– информационный объект хранится в собственной БД создавшей его АИС;

– существует программа, которая преобразует информационный объект в файл для контроля целостности и передачи в другие информационные системы с помощью КСУ. Это может быть прикладная АИС, которая его создает, хранит и обрабатывает. Однако для полноценного контроля целостности в ходе перемещения его между различными АИС потребуется программный модуль, входящий в состав программного обеспечения КСУ для выполнения подобного преобразования;

– показ пользователям объекта выполняется средствами прикладной АИС, работающей с данным объектом.

Каждый информационный объект КСУ должен обладать обязательным набором реквизитов, которые могут ею обрабатываться в процессе передачи между прикладными системами. Этот набор может включать данные АИС, создавшей объект, краткое описание объекта, данные для подсистем управления доступом, электронная подпись, метка целостности и т.д.

3.2. Учетные записи пользователей

Все работающие в институте или университете информационные системы коллективного пользования имеют свои базы данных учетных записей зарегистрированных пользователей. Помимо этого, существует общая база данных всех сотрудников – база домена. Это Active Directory в случае применения операционной системы (ОС) Windows или Astra Linux Directory для случая ОС Astra Linux, которая используется для идентификации и аутентификации сотрудников при входе в домен, а также для предоставления прав на действия в файловой системе, в том числе, для управления доступом к общим корпоративным ресурсам.

В случае применения КСУ становится более логичной реализация единой политики управления доступом - в частности, появляется возможность единого подхода к регистрации пользователей различных систем. БД пользователей КСУ должна содержать информацию о пользовательских группах таких, как структура подразделений учреждения с учетом их иерархии, группы доступа, списки рассылки и т.д., в ней должны храниться данные о ролях и пользователях, назначенных на эти роли, пользовательских привилегиях.

Существенная особенность учебных заведений, заметно влияющая на обеспечение информационной безопасности используемых в них АИС, состоит в том, что преподаватели и сотрудники институтов и университетов могут входить в несколько подразделений, причем это не отклонение от правил, а именно норма. Помимо подразделений в обычной иерархии – факультеты, кафедры и т.д., они могут входить в редакционные подразделения, ученые и диссертационные советы, подразделения, создаваемые для выполнения конкретных проектов и др. Эта особенность должна учитываться при проектировании БД пользователей КСУ, а также назначении прав доступа к информационным объектам как КСУ, так и прикладных АИС. Особое значение имеет эта особенность при реализации процедуры удаления учетной записи пользователя, т.к. ее удаление из одного

подразделения не должно приводить к удалению из всей БД, однако при этом должна сохраняться возможность и полного удаления всех данных пользователя из БД.

3.3. Управление доступом

Использование КСУ в случае, если передаваемая информация оформляется в виде ее объектов, позволяет реализовать единую систему управления доступом в рамках всего института, по крайней мере для пользователей, зарегистрированных в БД домена. Тогда для объектов КСУ списки доступа следует формировать с использованием идентификаторов единой базы данных института или университета. Такой подход позволяет автоматизировать назначение прав при передаче информации между разными системами, т.к. права на объект КСУ в принимающей системе пользователь, имеющий их в отправляющей, получит автоматически. В случае же передачи объекта другому пользователю в той же или в другой АИС достаточно просто дать ему необходимые права, которые автоматически преобразуются в права в принимающей системе. Разумеется, такое назначение прав может быть выполнено только пользователем, имеющим право модификации прав доступа для данного информационного объекта с точки зрения деловой логики отправляющей системы. Использование стандартизованных маршрутов движения объектов КСУ, ориентированных на решение типовых проблем и задач, позволит упростить работу пользователей системы в части модификации прав доступа.

Права доступа могут предоставляться с учетом положения сотрудника в должностной иерархии, например, руководитель может иметь право чтения, редактирования, а также модификации прав доступа информационных объектов своего подразделения. Возможность предоставления доступа к объектам КСУ не только конкретным пользователям, но и группам пользователей, а также указанным ролям, на которые может быть назначен пользователь, обеспечивает гибкое управление этим механизмом.

Согласно действующей нормативной базе (например, [9]), в АИС требуется «реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа», в частности, для работы с данными высокого уровня конфиденциальности может требоваться реализация мандатного разграничения.

Разграничение доступа по мандатной модели может быть реализовано тремя способами. Во-первых, данные разного уровня конфиденциальности могут быть разделены физически, т.е. обрабатываться в разных контурах локальной вычислительной сети, храниться на разных серверных компьютерах, доступ к ним осуществляется с разных клиентских рабочих мест. Тогда в рамках АИС или КСУ не требуется предусматривать каких-либо программных механизмов мандатного разграничения. Во-вторых, обработка данных всех уровней конфиденциальности может производиться на одних и тех же компьютерах с получением информации об этих уровнях от используемой ОС. При этом предполагается, что ОС предусматривает создание сеансов работы пользователей с разными уровнями конфиденциальности и этот уровень выбирается при входе в домен. В такой ситуации прикладная АИС при запуске клиентского приложения получает уровень конфиденциальности сеанса и использует его при дальнейшей работе для разграничения доступа к своим информационным объектам, в том числе к объектам КСУ. Ну и, наконец, мандатное разграничение доступа полностью реализуется средствами самой информационной системы, т.е. при входе пользователя в домен его сеансу работы присваивается максимальный доступный уровень конфиденциальности, а реальный уровень конфиденциальности, определяющий его права на действия с информационными объектами, выбирается им при работе в прикладной АИС. Такой подход предоставляет широкие возможности для различных действий сотрудников, например, при создании информационного объекта пользователь может сам указать его уровень конфиденциальности, отличный от уровня его сеанса работы. Однако следует отметить, что реализация такой логики сложна алгоритмически.

При реализации политики безопасности особое внимание следует обратить на такое действие, как уничтожение информационного объекта. В случае, когда информационный объ-

ект уничтожается его создателем вскоре после создания, это действие не вызывает особых вопросов. Ситуация существенно изменяется, когда информационный объект был передан в другие АИС, и с ним уже работает несколько пользователей. В этом случае процедура уничтожения объекта должна быть детально проработана как с точки зрения пользователя, имеющего право на инициализацию процесса уничтожения, так и алгоритма действий сотрудников, работающих с этими данными. Отдельно прорабатывается последовательность действий во внешних системах, которые работают с уничтожаемым объектом. Понятно, что наиболее полно и непротиворечиво все указанные действия могут быть реализованы только в случае внедрения КСУ.

3.4. Защита информации в точках взаимодействия систем

Основной задачей КСУ является обеспечение взаимодействия всех используемых АИС, следовательно, важен вопрос ведения протоколов безопасности в части совместной работы различных систем. В протокол безопасности заносятся и события, связанные с изменениями в базе данных пользователей: создание новых учетных записей, удаление устаревших, изменение прав пользователей, создание, удаление и изменение состава групп пользователей. Эти действия выполняются на уровне общей БД пользователей КСУ, следовательно, их протоколирование также должно выполняться с помощью ее механизмов.

Работа с электронными подписями и контроль целостности информационных объектов должны реализовываться средствами КСУ. Контроль целостности может быть реализован путем вычисления хэш-значений информационных объектов, хранения полученных хэш-значений в отдельной БД под управлением КСУ и проверки целостности по команде пользователей или автоматически в каких-либо критичных ситуациях, например, при импорте объекта КСУ, экспортированного из какой-либо АИС. Для полноценного внедрения усиленных ЭП [10] требуется формирование ключевой инфраструктуры, обеспечивающей хранение закрытых ключей пользователей, а также доступ к открытым ключам для проверки подписей. Все эти действия, а также регулярная замена криптографических ключей, наиболее естественно реализуются с помощью механизмов, встроенных в КСУ. Отметим, что в рамках единой системы, которой и является КСУ, может с успехом использоваться и простая ЭП, которая «посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом» [10].

В ряде случаев АИС, работающие в учебных или научных институтах, могут рассматриваться как объекты критической информационной инфраструктуры (КИИ), особенно это актуально для КСУ. Как указано в [11, 12], к таким объектам относятся, в частности, АИС, работающие в сфере науки, что, без сомнения, актуально для КСУ, работающей в учебном институте. Однако специальные меры по обеспечению безопасной работы таких систем предъявляются только к так называемым значимым объектам, т.е. к «объектам критической информационной инфраструктуры, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов критической информационной инфраструктуры» [11]. Категорирование объектов КИИ проводится в соответствии с [12], при этом учитываются возможные последствия от прекращения или нарушения функционирования объектов КИИ в социальной, экономической, политической, экологической и некоторых других сферах. В большинстве случаев нарушение функционирования АИС или КСУ в учебных институтах не может приводить к серьезным последствиям в этих областях, что позволяет не присваивать этим АИС категории значимости объектов КИИ.

Заключение

Цифровизация учебных заведений невозможна без решения ряда проблем, связанных с обеспечением информационной безопасности. Предложенное внедрение КСУ существенно видоизменяет эту задачу, но выигрыш в плане расширения функциональных возможностей всего компьютерного комплекса учебного заведения существенно перевешивает очевидные сложности этого процесса. Реализация систем класса КСУ позволяет сделать гораздо более логичными процессы обмена данными как

между работающими в учреждении АИС, так и между конкретными сотрудниками, работающими с этими системами. Такой подход дает возможность реализовать необходимые СЗИ: протоколирование, контроль целостности, управление доступом и т.д. В этом случае становится возможным полноценное внедрение простых и усиленных ЭП.

Предложенное решение позволяет изменить порядок администрирования всего программного обеспечения: сделать единую базу данных пользователей на основе базы данных домена, вести единый протокол безопасности, задавать права доступа ко всем обрабатываемым информационным объектам в терминах КСУ, что позволит автоматизировать управление доступом к объектам, передаваемым между различными АИС.

Признание информационных систем института или университета значимыми объектами КИИ существенно усложняет их разработку, ввод в действие и последующую эксплуатацию. Согласно [11, 12] для таких АИС требуется выполнение целого ряда требований в части применения в них СЗИ, периодическое тестирование механизмов защиты, а также взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Литература

1. Коваленко В.Е. Задачи анализа, планирования и оптимизации в АСУ ВУЗ. — М.: НИИВШ, 1980. — 40 с.
2. Электронная информационно образовательная среда ВУЗа (ЭИОС ВУЗа). https://www.tvoivyz.ru/.
3. Автоматизированная система управления высшим учебным заведением Федерального агенства морского и речного транспорта Минтранса РФ. https://asuvuz-msawt.gumrf.ru/.
4. Автоматизированная система управления учебным процессом ЮРГПУ (НПИ) имени М.И. Платова http://iasu.npi-tu.ru/.
5. Автоматизированная система управления (АСУ) вузом (учебным заведением, стузом, ссузом). http://www.kansoftware.ru/?sid=1.
6. Баймухамедов М.Ф., Скормин В.В.. Автоматизированная система управления вузом. https://articlekz.com/article/21022.
7. Примеры подсистем асу вуз. https://studfiles.net/preview/997094/page:12/.
8. Акимова Г.П., Даниленко А.Ю., Пашкина Е.В., Пашкин М.А., Подрабинович А.А., Соловьев А.В., Туманова И.В. Подход к автоматизации деловых процессов научной организации. Часть 2. Обеспечение информационной безопасности. // Системы высокой доступности. 2019. Т. 15. № 2. С. 20–31. DOI: 10.18127/j20729472-201902-02
9. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. / Приказ ФСТЭК России от 11 февраля 2013 г. № 17.
10. Об электронной подписи. Федеральный закон от 6 апреля 2011г. № 63-ФЗ.
11. Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".
12. Постановление Правительства РФ от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений".

Акимова Галина Павловна, в.н.с., ИСА ФИЦ ИУ РАН, к.т.н. Количество печатных работ: 60. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Даниленко Андрей Юрьевич, в.н.с., ИСА ФИЦ ИУ РАН, к.ф.-м.н., Количество печатных работ: 35. Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных.

Пашкина Елена Владимировна, ведущий программист, ИСА ФИЦ ИУ РАН. Количество печатных работ: 15. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: pashkina@isa.ru

Пашкин Матвей Александрович, н.с., ИСА ФИЦ ИУ РАН. Количество печатных работ: 20. Область научных интересов: системное программирование, информационные технологии, информационно-аналитические системы, электронный архив. E-mail: pashkin@isa.ru

Подрабинович Андрей Александрович, ведущий программист, ИСА ФИЦ ИУ РАН. Количество печатных работ: 10. Область научных интересов: системное программирование, проектирование и создание методов и программных средств управления электронными документами, защита информации в документооборотных системах. E-mail: podrabinovich@isa.ru

Соловьев Александр Владимирович, заместитель директора ИСА ФИЦ ИУ РАН по научной работе. Доктор технических наук. Количество печатных работ: 75. Область научных интересов: системный анализ, системы управления базами данных, теория надежности, математическое моделирование, электронный документооборот, электронный архив, долговременное хранение электронных документов. E-mail: soloviev@isa.ru

Туманова Ирина Владимировна, ведущий программист, ИСА ФИЦ ИУ РАН. Количество печатных работ: 5. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив, имеет более 5 публикаций. E-mail: tumanova-irin@mail.ru

Ensuring Safety in the digitalization of Educational Institutions

G.P. Akimova, A.Yu. Danilenko, E.V. Pashkina, M.A. Pashkin, A.A. Podrabinovich, A.V. Soloviev, I.V. Tumanova

Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia

Abstract. The article describes the features of the work of higher educational institutions, including business processes in these structures. The conclusion was made about the need for digitalization not of individual areas of work, but of all the activities of an institute or university, the expediency of solving this problem was justified by introducing a unified information system that would combine all currently used and promising automated information systems. The issues of information security in the implementation of this decision are considered.

Keywords: higher education institution, information security, organization business processes, digitalization, automated information systems.

DOI 10.14357/207186321904010

References

1. Kovalenko V.Ye. Zadachi analiza, planirovaniya i optimizatsii v ASU VUZ. — M.: NIIVSH, 1980. — 40 s. [Kovalenko V.E. The tasks of analysis, planning and optimization in the ACS of the university].
2. Elektronnaya informatsionno obrazovatel'naya sreda VUZa (EIOS VUZa)/ [Electronic educational information environment of the university (EIOS of the university)]/ https://www.tvoivyz.ru/.
3. Avtomatizirovannaya sistema upravleniya vysshim uchebnym zavedeniyem Federal'nogo agenstva morskogo i rechnogo transporta Mintransa RF. [Automated management system of a higher educational institution of the Federal Agency for Sea and River Transport of the Ministry of Transport of the Russian Federation]. https://asuvuz-msawt.gumrf.ru/.
4. Avtomatizirovannaya sistema upravleniya uchebnym protsessom YURGPU(NPI) imeni M.I. Platova. [The automated educational process management system of the SRSPU (NPI) named after M.I. Platova]. http://iasu.npi-tu.ru/.
5. Avtomatizirovannaya sistema upravleniya (ASU) vuzom (uchebnym zavedeniyem, stuzom, ssuzom). [Automated control system (ACS) of the university (educational institution, college, collegiate)]. http://www.kansoftware.ru/?sid=1.
6. Baymukhamedov M.F., Skormin V.V. Avtomatizirovannaya sistema upravleniya vuzom. [M.F. Baimukhamedov, V.V. Skormin. Automated university management system]. https://articlekz.com/article/21022.
7. Primery podsistem asu vuz. [Examples of ASU university subsystems]. https://studfiles.net/preview/997094/page:12/.
8. Akimova G.P., Danilenko A.YU., Pashkina Ye.V., Pashkin M.A., Podrabinovich A.A., Solov'yev A.V., Tumanova I.V. 2019. Podkhod k avtomatizatsii delovykh protsessov nauchnoy organizatsii. Chast' 2. Obespecheniye informatsionnoy bezopasnosti.[Akimova G.P., Danilenko A.Yu., Pashkina E.V., Pashkin M.A., Podrabinovich A.A., Soloviev A.V., Tumanova I.V. Approach to automate business processes of scientific organization. Part 2. Information security.] Sistemy vysokoy dostupnosti. [High availability systems]. 2: 20-31.
9. Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh. [On the approval of requirements for the protection of information that is not a state secret contained in state information systems]. Prikaz FSTEK Rossii ot 11 fevralya 2013 g. № 17. [Order of the FSTEC of Russia dated February 11, 2013 №. 17].
10. Ob elektronnoy podpisi. Federal'nyy zakon ot 6 aprelya 2011g. № 63-FZ. [About electronic signature. Federal Law of April 6, 2011 №. 63-FZ].
11. Federal'nyy zakon ot 26.07.2017 N 187-FZ "O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii". [Federal Law of 26.07.2017 № 187-ФЗ “On the Security of the Critical Information Infrastructure of the Russian Federation”].
12. Postanovleniye Pravitel'stva RF ot 8 fevralya 2018 g. № 127 "Ob utverzhdenii Pravil kategorirovaniya ob"yektov kriticheskoy informatsionnoy infrastruktury

Rossiyskoy Federatsii, a takzhe perechnya pokazateley kriteriyev znachimosti ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy". [Decree of the Government of the Russian Federation of February 8, 2018 № 127 "On approval of the Rules for the categorization of objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of the criteria of significance of objects of critical information infrastructure of the Russian Federation and their values"].

G.P. Akimova – Ph.D.(Eng.), Leading Research Scientist, Institute for Systems Analysis of FRC CSC RAS (Moscow, Russia) E-mail: akimova@isa.ru

A.Yu. Danilenko – Ph.D.(Phys.-Math.), Leading Research Scientist, Institute for Systems Analysis of FRC CSC RAS (Moscow, Russia) E-mail: danilenko@isa.ru

E.V. Pashkina – Leading Programmer, Institute for Systems Analysis of FRC CSC RAS (Moscow, Russia)

E-mail: pashkina@isa.ru

A.A. Podrabinovich – Leading Programmer, Institute for Systems Analysis of FRC CSC RAS (Moscow, Russia) E-mail: podrabinovich@isa.ru

M.A. Pashkin – Research Scientist, Institute for Systems Analysis of FRC CSC RAS (Moscow, Russia)

E-mail: pashkin@isa.ru

A.V. Solovev – Dr.Sc.(Eng.), Main Research Scientist, Institute for Systems Analysis of FRC CSC RAS (Moscow, Russia) E-mail: soloviev@isa.ru

I.V. Tumanova – Leading Programmer, Institute for Systems Analysis of FRC CSC RAS (Moscow, Russia)
E-mail: tumanova-irin@mail.ru