



**Басыров Р. Р., Паршин К. А.**

# **АНАЛИЗ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ В УЧЕБНОМ ЗАВЕДЕНИИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА**

*Статья посвящена рассмотрению проблем в области информационной безопасности, возникающих при внедрении в образовательном учреждении системы электронного документооборота. В статье поставлены основные технические и организационные задачи, решение которых требуется для организации защищенной системы электронного документооборота (ЭДО). Определен порядок решения поставленных задач. Обозначены проблемы, связанные с автоматизацией процессов по обработке информации ограниченного доступа.*

**Ключевые слова:** документ, информация, угроза, документооборот, защита информации, общедоступная информация, информация ограниченного доступа, персональные данные, коммерческая тайна.

**Basyrov R. R., Parshin K. A.**

# **ANALYSIS OF INFORMATION SECURITY PROBLEMS AT IMPLEMENTATION OF EDM SYSTEM IN EDUCATIONAL INSTITUTION**

*The article considers the problems of information security arising from the implementation of an educational institution electronic document management system. In the article estab-*

lished the basic technical and organizational tasks that is required for secure EDM system. The procedure for solving problems. The problems related to the automation of processes for the processing of restricted information.

**Keywords:** document, information, threat, document management, information security, public information, restricted information, personal data, trade secrets.

При внедрении в организации новых информационных систем зачастую возникает проблема выбора программно-аппаратного комплекса, на котором данная система спроектирована. Проблема выбора программно-аппаратной базы в первую очередь обусловлена основным направлением деятельности организации: выпускаемой продукцией или предоставляемыми услугами, основными производственными процессами, информационными потоками, циркулирующими в организации. Во-вторых, уже существующими информационными системами, с которыми необходимо осуществлять взаимодействие: проектирование и разработка процессов обмена информацией между системами, организация единого пространства пользователей и их каталогов, синхронизация данных, используемых совместно всеми системами. В-третьих, законодательством, устанавливающим жесткие требования, предъявляемые к информационным системам, на основе информации, обрабатываемой в таких системах.

Внедрение информационной системы электронного документооборота в государственном образовательном учреждении не является исключением и также ставит перед руководством проблему выбора программно-аппаратной базы, на которой данная система будет разработана. Во многом это обусловлено большим количеством информационных потоков и разнородностью информации, циркулирующей в них. Сюда относится служебная информация делового характера, необходимая для организации работы всех структурных подразделений, и информация ограниченного доступа: персональные данные сотрудников и студентов, информация, составляющая коммерческую тайну. Помимо этого, стоит отметить проблему взаимодействия между системой ЭДО и теми функционирующими системами, которые уже занимаются обработкой данных информационных потоков [1, 2, 5].

Таким образом, проблема выбора строится из нескольких ключевых вопросов, которые необходимо решить для достижения конечной цели – запуск полностью функционирующей системы ЭДО и перевод организации на безбумажное делопроизводство.

Основными задачами информационной безопасности, требующими решения в первую очередь, являются:

1) определить основные потоки информации и маршруты их следования между структурными подразделениями организации;

2) определить, какие виды информации циркулируют в этих потоках;

- какая общедоступная информация циркулирует в системе;

- какие виды информации ограниченного доступа циркулируют в системе;

3) определить, какие процессы по обработке информации производятся в организации, и какая при этом информация формируется;

4) определить, какие процессы обычного бумажного делопроизводства будут автоматизироваться и, как следствие, какая информация будет циркулировать в системе ЭДО;

5) определить, с какими существующими информационными системами, функционирующими в организации, будет взаимодействовать система ЭДО, и какими данными они будут обмениваться;

6) определить, какие меры и средства защиты информации необходимо использовать для обеспечения информационной безопасности.

Схема организации защищенной системы ЭДО представлена на рисунке 1.

При этом наиболее важной и ключевой задачей, влияющей на непосредственный выбор программно-аппаратной базы, является определение всех процессов по обработке информации ограниченного доступа, и принятие решений, будут ли эти процессы автоматизироваться и переводиться в систему ЭДО.

Автоматизация с помощью системы ЭДО процессов по обработке информации ограниченного доступа, таких как коммерческая тайна и персональные данные, влияет на требования по защите информации, предъявляемые к информационным системам. Помимо основных задач по технической организации необходимых мер, поднимаются вопросы о наличии разграничения между функциональ-

# Средства защиты информации

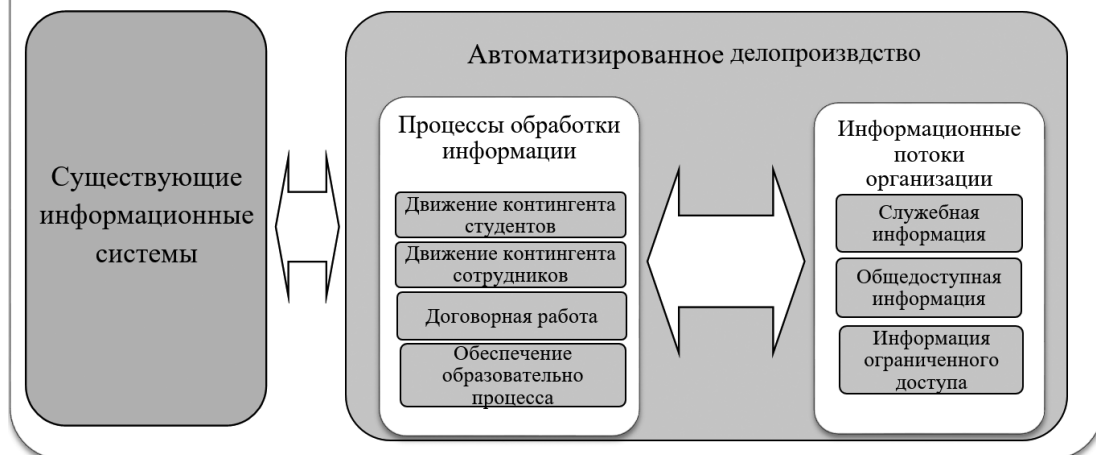


Рис 1. Схема организации защищенной системы ЭДО.

ными модулями системы, обрабатывающими как с информацией ограниченного доступа, так и общедоступную информацию, необходимую для работы сотрудников организации. Также возникает ряд вопросов, касающихся администраторов системы, которые в силу своих должностных обязанностей получают практически неограниченный доступ ко всем данным, обрабатываемым в системе [6, 7].

В случае если система ЭДО автоматизирует весь процесс делопроизводства учебного учреждения, возникает ряд проблем, в первую очередь связанных с тем, что информация ограниченного доступа разных видов циркулирует в единых информационных потоках и обрабатывается едиными механизмами. Таким образом, для реализации информационной безопасности в полной мере, в соответствии с требованиями законодательства,

необходимо применять методы и средства защиты каждой категории информации ограниченного доступа комплексно по отношению ко всей системе. Иными словами, как только в системе начинает обрабатываться информация, содержащая персональные данные, вся система автоматически становится ИСПДН, а это накладывает дополнительные требования по средствам защиты и требованиям, устанавливаемым законодательством Российской Федерации [1–5].

Исходя из всего вышеизложенного, можно сделать вывод об актуальности разработки единой модели, описывающей архитектуру построения, требования по защите, а также актуальные методы и средства информации в зависимости от того или иного вида информации ограниченного доступа, которые будут обрабатываться в системах ЭДО.

## Примечания

1. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.
2. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
3. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
6. Положение «О порядке обработки и защиты персональных данных работников и лиц, обучающихся в университете».

**БАСЫРОВ Руслан Равильевич**, программист 2 категории Управления информатизации, отдел АСУФР, Уральский государственный университет путей сообщения, 620034, Свердловская обл., г. Екатеринбург, ул. Колмогорова, 66. E-mail: RRBasyirov@usurt.ru

**ПАРШИН Константин Анатольевич**, к.т.н, доцент кафедры «Информационные технологии и защита информации», Уральский государственный университет путей сообщения, 620034, Свердловская обл., г. Екатеринбург, ул. Колмогорова, 66. E-mail: KParshin@usurt.ru

**BASYROV Ruslan**, Programmer 2 categories of Informatization directorate, Department ASUFR, Ural State University of Railway Transport, 620034, Sverdlovsk region, Ekaterinburg, Kolmogorov street, 66. E-mail: RRBasyirov@usurt.ru

**PARSHIN Konstantin**, PhD, associate professor of «Information technologies and protection of information», Ural State University of Railway Transport, 620034, Sverdlovsk region, Ekaterinburg, Kolmogorov street, 66. E-mail: KParshin@usurt.ru