

УДК 004.032.2

*Н.О. Кузнецова, Т.К. Кириллова, Д.И. Майоренко*

*Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

## **ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕДИНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ФГБОУ ВО ИРГУПС**

**Аннотация.** В статье рассмотрена работа Единой информационной системы ФГБОУ ВО ИРГУПС, с точки зрения организации работы персональных данных. Единая информационная система представляет собой совокупность информации, информационных технологий и технических средств, с помощью которых обеспечивается формирование, обработка, хранение информации, а также ее предоставление.

Показаны средства защиты информации в Единой информационной системе. Описаны организационные и технические меры защиты информации.

Выявлены преимущества и недостатки системы электронного документооборота. Для устранения недостатков были предложены рекомендации по улучшению Единой информационной системы в рамках функционирования системы электронного документооборота.

**Ключевые слова:** единая информационная система, персональные данные, система электронного документооборота.

*N.O. Kuznetsova, T.K. Kirillova, D.I. Mayorenko*

*Irkutsk State Transport University, Irkutsk, the Russian Federation*

## **ORGANIZATION OF PERSONAL DATA PROCESSING IN A UNIFIED INFORMATION SYSTEM**

**Abstract.** The article discusses the work of the Unified Information System of the Irkutsk State Transport University, from the point of view of organizing the work of personal data. A unified information system is a collection of information, information technologies and technical means, with the help of which the formation, processing, storage of information, as well as its provision is ensured.

The means of information protection in the Unified Information System are shown. The organizational and technical measures to protect information are described.

The advantages and disadvantages of the electronic document management system are revealed. To eliminate the shortcomings, recommendations were proposed to improve the Unified Information System within the framework of the functioning of the electronic document management system.

**Keywords:** unified information system, personal data, document management system.

### **Введение**

Современные требования к обработке персональных данных имеют ряд особенностей, обусловленных изменениями в законодательстве, регулирующих систему электронного документооборота (СЭД) и наличие технического обеспечения. Цель исследования – проанализировать работу информационной системы ФГБОУ ВО ИРГУПС в рамках функционирования СЭД.

В конце 2020 года вышли новые поправки в Федеральный закон №152 «О персональных данных». Изменения вступили в силу с 1 марта 2021 года. Изменились требования к обработке и защите персональных данных [1]. По решению Государственной думы ужесточены меры ответственности за неправомерную обработку персональных данных. Размер административного штрафа по статье 13.11 КоАП РФ возрос в два раза [2]. Данные изменения касаются большинства юридических лиц, поскольку в значительной части организаций накапливаются, хранятся или каким-то образом используются в работе персональные данные. Соответственно, данные организации являются операторами персональных данных.

Крупные организации имеют систему электронного документооборота, и процедура обработки персональных данных четко регламентирована. Система предназначена для осуществле-

ния коллективной работы над документами, осуществления их визирования и согласования. Документы, которые попадают в эти системы для обработки, содержат персональные данные сотрудников компании и иных лиц.

### **Поправки в Федеральный закон «О персональных данных»**

Согласно поправкам Федерального закона «О персональных данных», пункт 10 признан утратившим силу – аннулируется понятие «общедоступные персональные данные». Окончательно принято правило – «любую личную информацию о субъекте можно размещать только с его прямого согласия». Появилось новое понятие – «персональные данные, разрешенные субъектом для распространения». Согласно закону, к разрешенным для распространения ПДн относятся те персональные данные, к которым самим субъектом ПДн предоставлен доступ неограниченного круга лиц. Доступ предоставляется путем дачи согласия на обработку персональных данных, которые разрешены субъектом для распространения в порядке, предусмотренном ФЗ. Соответственно, изменились требования к содержанию согласия на обработку персональных данных.

В законе вводится понятие отдельного письменного согласия при распространении персональных данных субъектов. То есть каждая организация, размещающая персональные данные работников, клиентов, граждан на сайте, иных Интернет-ресурсах, обязана после 1 марта получить отдельное согласие и тем самым отказаться от укоренившейся практики так называемых «общих» согласий. Каждая компания, которая использовала персональные данные граждан, взяв их из открытых источников, должна также получить отдельное согласие гражданина (субъекта персональных данных).

### **Механизм осуществления обработки персональных данных во ФГБОУ ВО ИРГУПС**

Рассмотрим механизм осуществления обработки персональных данных в ФГБОУ ВО ИРГУПС. Данная организация использует в своей работе СЭД. Любая система электронного документооборота, которая имеет в своем составе справочники сотрудников организации, клиентов и контрагентов, содержит и персональные данные. То есть СЭД выступает как часть информационной системы персональных данных (ИСПДн). В терминах государственных стандартов по информационным технологиям ИСПДн – это автоматизированная система, а СЭД выступает в качестве программного продукта (часть комплекса технических средств, средство вычислительной техники). Закон требует приведения в соответствие требованиям именно ИСПДн заказчика, как оператора персональных данных.

К системе электронного документооборота (как и к информационной системе персональных данных) выдвигаются различные требования в рамках выполнения 152-ФЗ. Требования зависят:

- от результатов обследования и классификации ИСПДн: в зависимости от них может потребоваться применение сертифицированных средств защиты информации от несанкционированного доступа (СЗИ НСД) и/или средств криптографической защиты информации (СКЗИ);

- от устройства СЭД (как программного продукта, так и автоматизированной системы предприятия): СЭД предприятия может использовать как внешние, так и встроенные средства защиты.

Электронный документооборот функционирует в нескольких системах:

- Информационная система «Единая информационная система» (ЕИС);
- «1С: Зарплата и Кадры» и «1С: Бухгалтерия»;
- Внешние сервисы («Контур.Экстерн», «Контур.Диадок», ЕИС «Госзакупки»).

Единая информационная система обеспечивает формирование, обработку, хранение информации, а также ее передачу. ЕИС представляет собой совокупность информации, информационных технологий и технических средств. ЕИС состоит из следующих подсистем (рисунки 1):



**Рис. 1. Состав Единой информационной системы**

Таким образом, ЕИС – это распределённая информационная система, в которой присутствует разграничение прав доступа пользователей [3], в зависимости от того, кем является пользователь системы (обучающийся, преподаватель, работник).

Согласно заключения акта обследования системы, проведенного сотрудниками ФГБОУ ВО ИрГУПС, для ЕИС определена необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке. Требования к техническим средствам защиты ЕИС должны обеспечивать этот уровень защищенности [4].

Для обеспечения функционирования ЕИС используются следующие программные, программно-аппаратные средства защиты информации (СЗИ), таблица 1:

Таблица 1. Средства защиты информации ЕИС

№ п/п	Наименование программного, программно-аппаратного СЗИ	Функциональное описание
1	VPN L2TP	Протокол L2TP/IPsec обеспечивает процесс шифрования и расшифровки внутри ядра и поддерживает многопоточность.
2	VPN GRE	Протокол туннелирования, который позволяет инкапсулировать широкий спектр протоколов сетевого уровня в point-to-point каналах. Туннель GRE используется, когда пакеты должны быть отправлены из одной сети в другую через Интернет или незащищенную сеть.
3	VPN OPENVPN	Протокол OpenVPN отвечает за поддержание коммуникации между клиентом и сервером. Используется для создания защищенного “туннеля” между VPN-клиентом и VPN-сервером.
4	Microsoft Forefront Threat Management Gateway	Прокси-сервер для защиты сети от атак извне, а также контроля интернет-трафика. Выполняет функции интегрированного шлюза, обеспечивающего сетевую безопасность.

Для обеспечения безопасности персональных данных при разработке и обслуживании системы существует политика доступа к базам данных. Она реализуется в рамках парольной политики, регламентирующей права доступа пользователей в систему электронного документооборота. В качестве средства авторизации применяется механизм доступа с помощью домена Microsoft Server, разграничивающего права и полномочия пользователя [5], в соответствии с внутренним положением ФГБОУ ВО ИрГУПС «Об организационных и технических мерах защиты персональных данных», политикой университета в области защиты персональных данных и перечнем лиц, допущенных к процессу обработки персональных данных.

Техническая реализация подразумевает систему личных кабинетов (обучающегося, сотрудника, преподавателя), обезличивание персональных данных, отображаемых техническому персоналу при обслуживании и проектировании системы [4], использования усиленной неквалифицированной электронной подписи, выпускаемой университетом средствами Microsoft Server.

Для обеспечения соответствия изменениям ФЗ были разработаны и введены в оборот согласия на обработку и передачу ПДн, согласие на использование изображения физического лица. Данные согласия были введены в структуру данных Единой информационной системы.

С точки зрения выполнения организационных мер, внедрен и функционирует следующий механизм.

1. Приказом ректора университета утверждено соглашение о признании электронной подписи, выпускаемой университетом. Таким образом, принимая данное соглашение, сторона взаимодействия (студент, сотрудник, преподаватель), признает юридически значимым электронный документооборот, осуществляемый в СЭД университета.

2. Стороны, использующие СЭД, могут применять электронную подпись как для шифрования данных и обеспечения аутентификации лица, при доступе к сервисам СЭД, так и для шифрования данных.

Вышеописанный механизм дает возможность регулярной актуализации форм согласий об обработке персональных данных, возможность организации единого места хранения данных согласий, возможность их отзыва по требованию, либо по окончанию правовых отношений сторон, что обеспечит своевременность уничтожения персональных данных по достижению целей обработки [5].

Еще одной сильной стороной решения является возможность контроля наличия согласия об обработке персональных данных субъекта, и обеспечивает возможность своевременного сбора согласий (при их отсутствии по какой-либо причине).

В качестве обеспечительной правовой меры при выпуске электронной подписи университета выступает удостоверение личности владельца электронной подписи [6,7], осуществляемого отделом кадров (преподаватели, работники) и студенческим сектором отдела кадров (обучающиеся). Технической мерой защиты служит использование простой электронной подписи (пары «пароль и логин»), выдаваемой каждому участнику электронного взаимодействия в СЭД при его регистрации в корпоративной сети.

### **Заключение**

Проведенный анализ выявил недостатки системы электронного документооборота:

1. Система не реализована в полной мере. В настоящий момент, в рамках функционирования СЭД реализовано несколько отдельных систем (в том числе, ЕИС), но они не организованы в едино-функционирующую систему электронного документооборота;

2. Не все работники обучены для работы с системой. Большая часть сотрудников обучены работе с ЕИС, но возникают ситуации, когда у работника возникают трудности при работе с системой.

Рекомендации по структурированию системы электронного документооборота:

Во-первых, для решения вопроса полноценной работы СЭД рекомендуется настроить маршрутизацию потока документов [8]. Во-вторых, стоит четко определить сотрудников, которые будут задействованы при работе с системой. И для сотрудников провести комплексное обучение с помощью средств электронного обучения (Moodle).

### **БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. РОСКОНАДЗОР. Об актуальных изменениях законодательства в сфере персональных данных Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» [Электронный ресурс]. URL: <https://74.rkn.gov.ru/news/news287270.htm#:~:text=01%20марта%202021%20года%20вступает,субъектом%20персональных%20данных%20для%20распространения> (дата обращения 27.01.2022г)

2. Кодекс Российской Федерации об административных правонарушениях. [Электронный ресурс]. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_34661/](http://www.consultant.ru/document/cons_doc_LAW_34661/) (дата обращения 27.01.2022г)

3. Бобылева М.П. Управленческий документооборот: от бумажного к электронному. Вопросы теории и практики. // Москва: Термика. 2013. – 26 с.

4. Анацкая А. Г. Защита электронного документооборота: учебное пособие / А. Г. Анацкая – Омск: СибАДИ, 2019. – 87 с.

5. Положение ФГБОУ ВО ИрГУПС «Об организационных и технических мерах защиты персональных данных». – Иркутск: Изд-во ИрГУПС.

6. Воробьев Е. Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: учебное пособие / Е. Г. Воробьев. – 3-е изд., перераб. – Санкт-Петербург: Интермедия, 2017. – 432 с.

7. Куняев Н. Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н. Н. Куняев; под редакцией Н. Н. Куняева. – 2-е изд., перераб. и доп. – Москва: Логос, 2020. – 500 с.

8. Скрипник Д. А. Обеспечение безопасности персональных данных: учебное пособие / Д. А. Скрипник. – 2-е изд. – Москва : ИНТУИТ, 2016. – 121 с.

### **REFERENCES**

1. ROSKOMNADZOR. On current changes in legislation in the field of personal data Federal Law No. 519-FZ dated 30.12.2020 "On Amendments to the Federal Law "On Personal Data" [Electronic resource]. Available at: <https://74.rkn.gov.ru/news/news287270.htm#:~:text=01%20mart%202021%20year%20year,subj>

ect%20personal%20data%20for%20distribution (accessed 10.09.2021) 2. The Code of Administrative Offences of the Russian Federation. Available at: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_34661/](http://www.consultant.ru/document/cons_doc_LAW_34661/) (Accessed 25 January 2022).

2. Code of the Russian Federation on administrative offenses. Available at: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_34661/](http://www.consultant.ru/document/cons_doc_LAW_34661/) (Accessed 25 January 2022).

3. Bobyleva M.P. Management document flow: from paper to electronic. Questions of theory and practice. // Moscow: Thermika. 2013.

4. Anatskaya A.G. Protection of electronic document management: a tutorial / A.G. Anatskaya. - Omsk: Si-badi, 2019. – 87 p.

5. Regulations of the Irkutsk State Transport University «On organizational and technical measures for the protection of personal data». – Irkutsk: ISTU.

6. Vorobiev E.G. Ensuring the security of personal data during their processing in personal data information systems: a tutorial / E.G. Vorobiev. - 3rd ed., Rev. - St. Petersburg: Intermedia, 2017. – 432 p.

7. Kunyaev N. N. Confidential office work and secure electronic document management: textbook / N. N. Kunyaev; edited by N. N. Kunyaev. - 2nd ed., Rev. and add. - Moscow: Logos, 2020. – 500 p.

8. Skripnik D.A. Ensuring the security of personal data: a tutorial / D.A. Skripnik. - 2nd ed. - Moscow: INTUIT, 2016. – 121 p.

#### **Информация об авторах**

*Кузнецова Надежда Олеговна* – студент группы БИМ.1-20-1, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: [kuznecova\\_no@irgups.ru](mailto:kuznecova_no@irgups.ru)

*Кириллова Татьяна Климентьевна* – к. э. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: [kirillova\\_tk@irgups.ru](mailto:kirillova_tk@irgups.ru)

*Майоренко Данила Иванович* – начальник отдела информационной безопасности и электронного документооборота, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: [mayorenko\\_di@irgups.ru](mailto:mayorenko_di@irgups.ru)

#### **Information about the author**

*Nadezhda Olegovna Kuznetsova* – Student, Irkutsk State Transport University, Irkutsk, e-mail: [kuznecova\\_no@irgups.ru](mailto:kuznecova_no@irgups.ru)

*Tatyana Klimentievna Kirillova* – Candidate of Economic Sciences, Irkutsk State Transport University, Irkutsk, e-mail: [kirillova\\_tk@irgups.ru](mailto:kirillova_tk@irgups.ru)

*Danila Ivanovich Mayorenko* – Irkutsk State Transport University, Irkutsk, e-mail: [mayorenko\\_di@irgups.ru](mailto:mayorenko_di@irgups.ru)