СТАТЬЯ

УДК 004.05

СТАНДАРТИЗАЦИЯ МОДЕЛЕЙ ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сысоева Л.А.

ФГБОУ ВО «Российский государственный гуманитарный университет», Москва, e-mail: Leda@rggu.ru

Современный этап цифровизации организаций характеризуется постоянным расширением спектра деловых процессов, реализуемых на основе автоматизированных информационных систем, что вызывает и увеличение объемов персональных данных, обрабатываемых информационными системами. В 2021 году набор стандартов в сфере информационной безопасности пополнил ГОСТ ISO/IEC 29100-2021, одной из задач которого является стандартизация требований к мерам защиты персональных данных в информационных системах персональных данных (ИС ПДн). Цель исследования – определение моделей взаимодействия участников обработки персональных данных в информационных системах персональных данных и специфики их реализации на практике. В статье представлены факторы, обуславливающие необходимость стандартизации требований к мерам обеспечения безопасности персональных данных в ИС ПДн, связанные с тенденциями развития современных ИКТ и систем. В соответствии с рекомендациями стандарта определены процессы, которые необходимо выполнять при обработке персональных данных в ИС ПДн (обезличивание, маскирование, идентифицирование, разрешение/запрет на обработку), и роли участников обработки ПДн (субъект ПДн, оператор, обработчик, третья сторона). Представлена структура ИС ПДн с учетом категорий участников обработки персональных данных и их ролей. Определены функции участников обработки ПДн в ИС ПДн, модели их взаимодействия и примеры реализации. На примере структуры ИС ПДн, обеспечивающей выполнение процесса «Подача электронного заявления абитуриентом», показано, что в зависимости от маршрута реализации процесса участники обработки ПДн могут выполнять различные роли. Разработка моделей взаимодействия участников обработки ПДн при выполнении деловых процессов позволяет определить их роли, сформировать регламенты их взаимодействия, что особенно важно при реализации сквозных процессов в корпоративных и межведомственных информационных системах.

Ключевые слова: персональные данные; обработка персональных данных; информационные системы персональных данных; модели взаимодействия участников обработки персональных данных

STANDARDIZATION OF INTERACTION MODELS OF PARTICIPANTS IN PERSONAL DATA PROCESSING IN PERSONAL DATA INFORMATION SYSTEMS

Sysoeva L.A.

Russian State University for the Humanities, Moscow, e-mail: Leda@rggu.ru

The modern stage of digitalization of organizations is characterized by a constant expansion of the range of business processes implemented on the basis of automated information systems, which causes an increase in the volume of personal data processed by information systems. In 2021, the set of standards in the field of information security was supplemented by GOST ISO/IEC 29100-2021, one of the tasks of which is to standardize the requirements for measures to protect personal data in personal data information systems (IS PD). The purpose of the study is to determine the models of interaction between participants in the processing of personal data in IS PD and the specifics of their implementation in practice. The article presents the factors that make it necessary to standardize the requirements for measures to ensure the security of personal data in IS PD related to the trends in the development of modern ICT and systems. In accordance with the recommendations of the standard, the processes that must be carried out when processing personal data in the IS PD (depersonalization, masking, identification, permission/prohibition to process) and the role of participants in the processing of PD (PD subject, operator, processor, third party) are determined. The structure of the IP PD is presented, taking into account the categories of participants in the processing of personal data and their roles. The functions of participants in PD processing in PD IS, models of their interaction and implementation examples are defined. Using the example of the IS PD structure, which ensures the execution of the process "Submission of an electronic application by an applicant", it is shown that, depending on the process implementation route, PD processing participants can perform various roles. The development of models of interaction between participants in the processing of PD during business processes makes it possible to determine their roles, form regulations for their interaction, which is especially important when implementing processes in corporate and interdepartmental information systems.

Keywords: personal data; processing of personal data; personal data information systems; models of interaction of participants in personal data processing

Современный этап цифровизации организаций характеризуется постоянным расширением спектра деловых процессов, реализуемых на основе автоматизированных информационных систем. Данной тенденции свойственно как увеличение объема и расширение набора персональных данных (ПДн), которые включаются в обработку с использованием информационных систем, так и рост масштаба самих информационных систем. Поэтому актуальность обеспечения безопасности персональных

данных при обработке их в информационных системах возрастает с каждым годом.

В 2021 году набор стандартов в сфере информационной безопасности пополнил ГОСТ ISO/IEC 29100-2021 [1], определяющий «место организационных, технических и процедурных аспектов в общей структуре обеспечения безопасности персональных данных» [1, с. V]. Основной задачей стандарта является формирование требований к мерам защиты персональных данных в информационных системах персональных данных (ИС ПДн) с учетом ролей участников в обработке ПДн.

Принятие стандарта ГОСТ ISO/IEC 29100-2021 обусловлено рядом тенденций в сфере современных информационно-коммуникационных технологий (ИКТ) и систем:

- постоянное расширение спектра ИКТ, которые участвуют в обработке персональных данных (одной из причин является включение в обработку данных, относящихся к специальной категории, и биометрических данных, для которых требуются специализированные технологии);
- рост сложности архитектур ИС ПДн (многоуровневые архитектуры клиент-сервер);
- увеличение масштабов ИС ПДн (государственные, федеральные, ведомственные, отраслевые и др.);
- необходимость интеграции ИС ПДн различного масштаба при реализации деловых процессов (например, корпоративных и федеральных ИС, корпоративных и отраслевых ИС);
- повышение доли аутсорсинговых услуг в жизненном цикле ИС ПДн.

Вышеперечисленные факторы обуславливают необходимость стандартизации требований к мерам обеспечения безопасности персональных данных при их обработке в ИС ПДн.

Методологической основой стандарта является процессный подход [2; 3], на основе которого обработка персональных данных в ИС ПДн включает процессы проектирования, реализации, эксплуатации, обеспечения систем, обрабатывающих ПДн, т.е. все процессы, составляющие жизненный цикл информационной системы.

Нормативной базой для определения категорий персональных данных, обрабатываемых с использованием ИС ПДн, является ФЗ «О персональных данных» [4].

Цель исследования – определить модели взаимодействия участников обработки персональных данных в информационных системах персональных данных и специфику их реализации на практике.

Материалы и методы исследования

В соответствии с ГОСТ ISO/IEC 29100-2021 информация, относящаяся к персональным данным и обрабатываемая с помощью информационных систем, обладает рядом характерных ей свойств [1; 4]:

- анонимность (свойство информации, не позволяющее прямо или косвенно определить субъект ПДн);
- обезличенность (свойство информации, когда принадлежность ПДн конкретному субъекту ПДн невозможно определить без дополнительных сведений);
- идентифицируемость (свойство информации, обеспечивающее успешность прямой или косвенной идентификации субъекта ПДн).

Вышеперечисленные свойства персональных данных определяют процессы, которые требуется выполнять в ИС ПДн:

- обезличивание данных (набор действий, не позволяющих без дополнительных сведений определить принадлежность ПДн конкретному субъекту);
- маскирование данных (набор действий, затрудняющих понимание ПДн, посредством замены реальных данных фиктивными данными или произвольными символами);
- идентифицирование данных (действия, результатом которых является прямая или косвенная идентификация субъекта ПДн на основе имеющихся ПДн, включающая определение необходимого и достаточного набора свойств, которые могут отличать один субъект ПДн от другого на внутрисистемном описании субъекта, а также могут с достаточной надежностью дать возможность идентифицировать субъект);
- разрешение / запрет на обработку данных (фиксирование в ИС ПДн разрешения/запрета на действия с персональными данными и другой информацией, влияющей на обработку ПДн).

При обработке ПДн выделяют несколько категорий участников [1], таких как (рис. 1):

1) субъект ПДн (физическое лицо, чьи ПДн обрабатываются);

2) оператор ПДн («юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и/или осуществляющее обработку ПДн» [1, с. 4]);

3) обработчик ПДн (юридическое или физическое лицо, осуществляющее обработку ПДн от имени и в соответствии с регламентами оператора обработки ПДн);

4) третья сторона (юридическое или физическое лицо, уполномоченное оператором или обработчиком ПДн обрабатывать ПДн или переходящее в статус самостоятельного оператора ПДн после получения запрашиваемых ПДн).

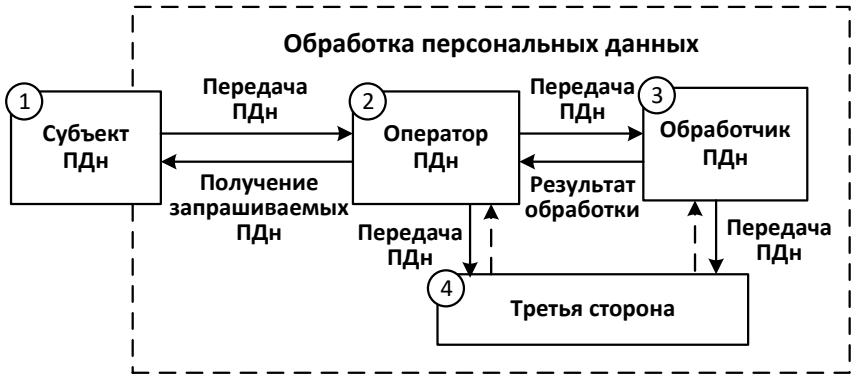


Рис. 1. Категории участников обработки персональных данных

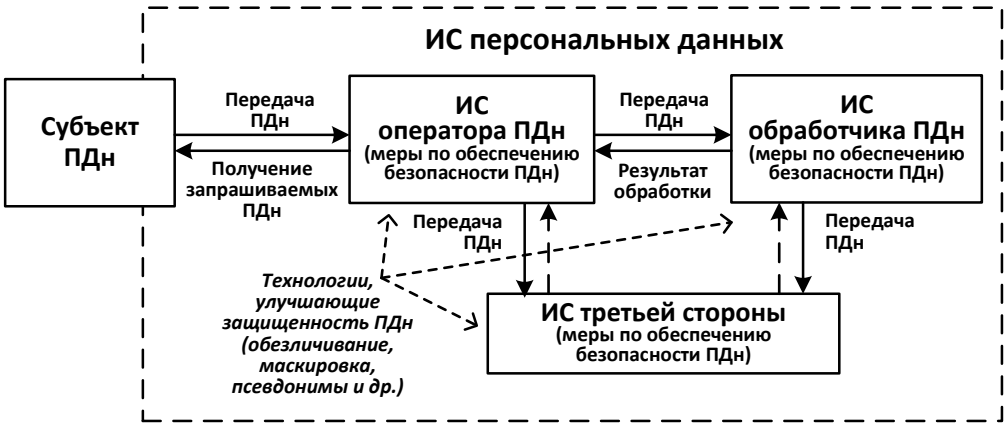


Рис. 2. Структура ИС ПДн с учетом участников обработки персональных данных и их ролей

Участники обработки ПДн выполняют свои функции с использованием информационных систем (рис. 2):

- ИС оператора ПДн;
- ИС обработчика ПДн;
- ИС третьей стороны.

В соответствии с ГОСТ ISO/IEC 29100-2021 во всех информационных системах, участвующих в обработке персональных данных, необходимо применять соответствующие меры по обеспечению безопасности ПДн с целью предотвращения нерегламентированной обработки ПДн без потери функциональности самих систем.

Для обеспечения защиты персональных данных в каждой ИС ПДн должны быть определены следующие компоненты, связанные с обработкой ПДн [1]:

- участники (субъекты обработки ПДн), их роли, функции;
- модели взаимодействия между участниками обработки ПДн;
- методы и технологии распознавания ПДн;
- требования к мерам обеспечения безопасности ПДн;
- политики обеспечения безопасности ПДн;
- меры обеспечения безопасности ПДн.

Рассмотрим более подробно модели взаимодействия между участниками обработки ПДн. При исследовании применяется процессный подход [2; 3] и рекомендации стандартов, регламентирующих обеспечение защиты персональных данных в ИС ПДн [1; 4].

Результаты исследования и их обсуждение

Первоначально определим функции участников обработки ПДн в ИС ПДн, которые необходимо учитывать при формировании моделей их взаимодействия (табл. 1).

Модели взаимодействия участников обработки персональных данных (субъекта ПДн, оператора, обработчика, третьей стороны) в ИС ПДн представлены в таблице 2.

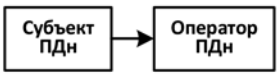
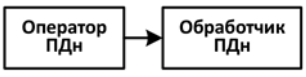
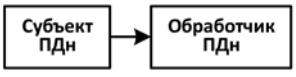
Таблица 1

Функции участников обработки ПДн

Участник обработки ПДн в ИС ПДн	Функции
Оператор ПДн	- Определяет цель (зачем) и способы (как) обработки ПДн. - Определяет минимально необходимый набор ПДн для достижения цели обработки. - Выполняет контроль за соблюдением принципов защиты ПДн во время обработки ПДн. - Определяет необходимость / возможность привлечения нескольких операторов ПДн при наличии нескольких целей обработки ПДн. - Определяет необходимость / возможность привлечения нескольких операторов ПДн для обработки одинаковых наборов ПДн. - Определяет необходимость / возможность привлечения нескольких операторов ПДн для одинаковых операций, выполняемых с ПДн. - Определяет необходимость / возможность передачи выполнения всех или части операций по обработке ПДн другим лицам от своего имени. - Осуществляет правовой контроль при реализации обработки ПДн и за деятельностью обработчика ПДн
Обработчик ПДн	- Выполняет обработку ПДн от имени оператора ПДн. - Обеспечивает соблюдение установленных оператором ПДн требований по защите ПДн. - Реализует соответствующие меры обеспечения безопасности ПДн, согласованные с оператором ПДн
Третья сторона	- Получает ПДн для обработки от оператора или обработчика ПДн. - Становится самостоятельным оператором ПДн после получения запрашиваемых персональных данных. - Самостоятельно осуществляет правовой контроль при реализации обработки ПДн

Таблица 2

Модели взаимодействия участников обработки ПДн в ИС ПДн

№	Модель взаимодействия	Графическая модель	Реализация
1	Субъект ПДн → Оператор ПДн		Подача запроса субъектом ПДн на оказание услуги оператору ПДн
2	Оператор ПДн → Обработчик ПДн		Передача ПДн оператором ПДн обработчику для выполнения определенных функций обработки ПДн на условиях соглашения об аутсорсинге
3	Субъект ПДн → Обработчик ПДн		Передача заявки субъектом ПДн на оказание услуги обработчику ПДн на условиях соглашения об аутсорсинге между оператором и обработчиком ПДн
4	Оператор ПДн → Субъект ПДн		Предоставление оператором ПДн результата обработки запроса субъекту ПДн (предоставление ПДн, относящихся к субъекту)
5	Обработчик ПДн → Субъект ПДн		Предоставление обработчиком ПДн результата выполнения обработки ПДн субъекту ПДн на условиях соглашения об аутсорсинге между оператором и обработчиком ПДн

Окончание табл. 2

№	Модель взаимодействия	Графическая модель	Реализация
6	Обработчик ПДн → Оператор ПДн	Обработчик ПДн → Оператор ПДн Предоставление ПДн	Предоставление обработчиком ПДн результата выполнения ИТ-сервиса оператору ПДн
7	Оператор ПДн → Третья сторона	Оператор ПДн → Третья сторона Передача ПДн	Передача оператором ПДн персональных данных для обработки третьей стороне в соответствии с заключенным соглашением при реализации сквозного процесса
8	Обработчик ПДн → Третья сторона	Обработчик ПДн → Третья сторона Передача ПДн	Передача обработчиком ПДн персональных данных для обработки третьей стороне в соответствии с регламентом обработки ПДн, определенным оператором ПДн

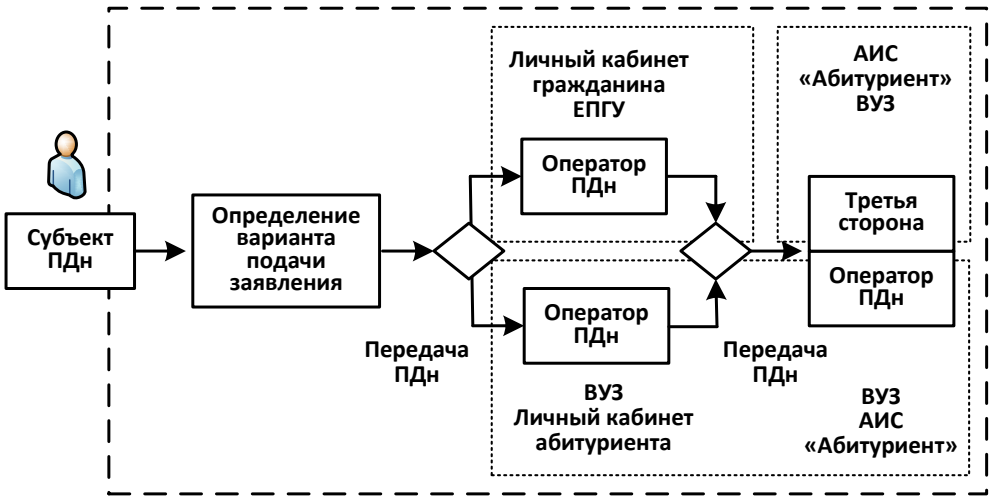


Рис. 3. Пример структуры ИС ПДн при реализации процесса «Подача электронного заявления абитуриентом»

Пример структуры ИС ПДн и выполняемых ролей участниками обработки персональных данных при реализации процесса «Подача электронного заявления абитуриентом» представлен на рисунке 3. Особенность процесса заключается в том, что если субъект ПДн подает заявление через единый портал государственных услуг (ЕПГУ), то в этом случае организация, сопровождающая ИС ЕПГУ, выполняет роль оператора ПДн, а вуз, сопровождающий АИС «Абитуриент», куда передаются ПДн абитуриента для дальнейшей обработки – третьей стороной. В случае когда субъект ПДн подает заявление через личный кабинет абитуриента, который является функциональным компонентом АИС «Абитуриент», роль оператора ПДн выполняет вуз.

Таким образом, разработка моделей взаимодействия участников обработки персональных данных при выполнении деловых процессов позволяет определить их роли, сформировать регламенты их взаимодействия, что особенно важно при реализации сквозных процессов [5] в корпоративных и межведомственных информационных системах.

Заключение

Использование рекомендаций стандарта ГОСТ ISO/IEC 29100-2021 для обеспечения безопасности ПДн в ИС ПДн позволит:

- улучшить меры защиты ПДн в ИС ПДн;

- стимулировать внедрение инновационных решений для обеспечения безопасности ПДн в ИС ПДн;

- унифицировать требования к мерам обеспечения безопасности ПДн в корпоративных и межведомственных информационных системах.

Список литературы

1. ГОСТ ISO/IEC 29100-2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных. Введ. 2021-11-30. М.: Стандартинформ, 2021. 21 с.

2. Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Манн, Иванов и Фербер, 2013. 544 с.

3. Франк Шёнталер, Готфрид Фоссен, Андреас Обервайс, Томас Карле. Бизнес-процессы: языки моделирования, методы, инструменты: практическое руководство / пер. с нем. М.: Альпина Паблишер, 2019. 264 с.

4. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_law_61801/ (дата обращения: 18.04.2022).

5. Сысоева Л.А. Стандартизация требований к прикладным информационным системам организации для включения их в единую систему управления документами // Научное обозрение. Технические науки. 2021. № 3. С. 55-60.