БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 55–68

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-2-55-68

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПРЕДПРИЯТИЯ*

Н.Е. КАРПОВА[1], А.А. БАБИНОВА[2]

[1] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность». E-mail: esib@samgtu.ru*
[2] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, ассистент кафедры «Прикладная математика и информатика». E-mail: anyuta.babinova2000@yandex.ru*

При современном развитии информационных технологий, ресурсов и компьютеризации общества во всём мире в каждой из сфер деятельности человека не обходится без информационных технологий. Некоторые из них уникальны и приносят доход своей уникальностью, и вследствие этого одной из наиболее более актуальных становится проблема обеспечения информационной безопасности в любых организациях и предприятиях, для любой сферы и бизнес-деятельности. Люди в связи со стремлением получить выгоду могут совершать преступные действия по отношению к источникам доходов, коими всегда является информация. Самым распространенным таким источником являются персональные данные. В любой организации и на любых предприятиях существуют угрозы безопасности информации, которая содержит персональные данные. Эта информация может быть утрачена, скопирована, изменена или заблокирована как злоумышленником из корыстных побуждений, так и допущенным персоналом по ошибке и неосторожности. Потеря конфиденциальной информации может повлечь как незначительный ущерб, так и весьма серьезные последствия. Поэтому важную роль в сохранении и улучшении деятельности организаций играет обеспечение безопасности персональных данных, так как эта проблема существует во всех сферах жизнедеятельности.

В настоящей статье рассмотрены вопросы, связанные с разработкой системы по обеспечению безопасности персональных данных в информационной системе предприятия. Во время выполнения работы были проанализированы нормативно-правовые акты в сфере защиты и обработки персональных данных в информационной системе предприятия, был осуществлен анализ существующих средств защиты и исходной защищенности ИСПДн.

* Статья получена 20 апреля 2024 г.

В результате выполнения работы была разработана система защиты персональных данных в ИСПДн. Был произведен выбор технических и организационных мер, а также обоснование оборудования для системы защиты.

Ключевые слова: персональные данные, конфиденциальная информация, информационная система персональных данных, информационные технологии, исходная защищенность, актуальные угрозы, нарушитель, меры по обеспечению безопасности, система защиты

ВВЕДЕНИЕ

В современном мире, где информационные технологии, ресурсы и компьютеризация общества играют ключевую роль, использование информационных технологий становится неотъемлемой частью всех сфер деятельности. Некоторые из этих технологий уникальны и приносят доход за счет своей уникальности. В связи с этим проблема обеспечения информационной безопасности в организациях и предприятиях, независимо от их сферы деятельности, становится одной из самых актуальных.

Из-за стремления людей к личной выгоде возникают ситуации, когда они совершают преступные действия в отношении источников дохода, которыми часто является информация. Одним из самых распространенных таких источников являются персональные данные. В любой организации и на любом предприятии существуют угрозы безопасности информации, содержащей персональные данные. Эта информация может быть потеряна, скопирована, изменена или заблокирована как злоумышленником из корыстных побуждений, так и по ошибке или неосторожности со стороны персонала. Потеря конфиденциальной информации может привести как к незначительным убыткам, так и к серьезным последствиям. Поэтому обеспечение безопасности персональных данных играет важную роль в сохранении и улучшении деятельности организаций, поскольку эта проблема актуальна во всех сферах жизнедеятельности.

Персональные данные обладают конкретной стоимостной ценностью, которая определяется как потенциальной прибылью от их использования, так и возможным ущербом от несанкционированного доступа. Затраты на обеспечение защиты таких данных постоянно растут, но компании стремятся избегать лишних расходов, предпочитая приобретать только необходимые решения для построения надежной системы защиты информации. Однако для оптимального выбора таких средств защиты необходима оценка их эффективности и соответствия требованиям конкретной ситуации, включая функциональные особенности и экономическую целесообразность.

Следует отметить, что обеспечение безопасности персональных данных в информационной системе предприятия требует не только обучения персонала, организации охраны объектов и других организационных мер по защите информации, но и выявления и изучения возможных каналов утечки данных, определения актуальных угроз, а также использования специализированных технических средств, способных противодействовать различным видам атак злоумышленников.

ИССЛЕДОВАНИЕ

Защита персональных данных регулируется Федеральным законом РФ от 27.07.2006 № 152 «О персональных данных». Он определяет основные термины и принципы обработки персональных данных физических и юридических лиц, а также предписывает требования по организации работы с такими данными для операторов и их ответственность в случае нарушения законодательства.

Для выполнения требований Закона «О персональных данных» было принято постановление Правительства Российской Федерации от 01.11.2012 № 1119 [3]. В пункте 4 этого документа установлено правило относительно выбора средств защиты персональных данных, согласно которому выбор таких средств должен соответствовать нормативным актам Федеральной службы по техническому и экспортному контролю (ФСТЭК) России.

Кроме этого, в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ [4] установление требований по защите ПД и контроль за их исполнением отнесен к компетенции ФСТЭК России.

В целях исполнения Закона «О персональных данных» [2] и постановления Правительства Российской Федерации от 01.11.2012 № 1119 [3] издан приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 [5], конкретизирующий состав и содержимое мер по обеспечению сохранности персональных данных.

Для оценки угроз информационной безопасности используется методика, утвержденная 5 февраля 2021 года Федеральной службой по техническому и экспортному контролю под названием «Методика оценки угроз безопасности информации» [7]. Этот документ опирается на классический подход к анализу угроз, который включает в себя идентификацию потенциальных рисков негативных последствий от угроз информационной безопасности, выявление источников этих угроз, оценку их возможностей и разработку сцена-

риев их реализации. Анализ проводится последовательно: определение рисков, выявление нарушителей, анализ их тактик и методов (разработка сценариев) и затем принятие решения о степени актуальности угрозы на основе этих данных.

В статье Гаврющенко А.П. «О методике определения актуальных угроз информационной безопасности с использованием БДУ ФСТЭК» рассмотрена методика оценки угроз безопасности, определены этапы определения актуальных угроз информационной безопасности, сопровождающиеся практическими примерами [9].

В качестве объекта исследования был выбран кабинет бухгалтерии АО «АИМ», имеющий площадь 40 квадратных метров и оснащеннный автоматизированными рабочими местами (АРМ). В нем установлены окна из ПВХ, а входная дверь выполнена из дерева.

Документы, обрабатываемые в ИСПДн, относятся к категории «иные персональные данные». Для обеспечения безопасности в системе бухгалтерии применяется антивирусное программное обеспечение Kaspersky Endpoint Security 11 и разграничение доступом в соответствии с политикой безопасности. Для обработки данных в ИСПДн используется программный комплекс 1С: Предприятие и 1С: Зарплата и управление персоналом. Также используется одно из клиентских приложений системы 1С: Предприятие – тонкий клиент.

После определения средств защиты ПДн в ИСПДн «Бухгалтерия» был определен уровень исходной защищенности согласно п. 2 «Методики» [8] ФСТЭК. Уровень исходной защищенности средний, так как не менее 70 % характеристик ИСПДн соответствуют уровню не ниже среднего.

Затем с помощью пункта 5.1.3 «Методики оценки угроз безопасности информации» [7] был составлен перечень актуальных нарушителей, среди них:

– персонал, поддерживающий работоспособность систем и сетей (администраторы, охранники, уборщики и прочие) (внутренний нарушитель);

– сотрудники, имеющие разрешение на использование систем и сетей (внутренний нарушитель).

После определения актуальных нарушителей следует определить уровни возможностей нарушителей, которые могут реализовывать угрозы безопасности информации. Уровни возможностей будем определять в соответствии с приложениями 8 и 9 к «Методике оценки угроз безопасности информации» [7]. Для этого были сопоставлены данные из указанного выше документа с перечнем актуальных нарушителей. Результаты сопоставления приведены в таблице.

Уровни возможностей актуальных нарушителей

№ п/п	Виды ущерба	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1: нарушение конфиденциальности персональных данных граждан	Персонал, поддерживающий работоспособность систем и сетей (администраторы, охранники, уборщики и прочие)	Внутренний	Н2
2		Сотрудники, имеющие разрешение на использование систем и сетей	Внутренний	Н1

Основным объектом атак является программное обеспечение 1С, поскольку оно служит для выполнения большинства задач пользователей.

Проанализируем неблагоприятные последствия, которые могут возникнуть в результате несанкционированного доступа к ресурсам 1С:

– раскрытие личных данных сотрудников, включая их адреса и контактную информацию, может привести к нежелательному вмешательству в их частную жизнь;

– несанкционированное изменение личных данных сотрудников может привести к внесению неверной информации в официальные документы, такие как приказы, распоряжения, заявления и т. д.;

– несанкционированное изменение информации о заработной плате и премиях сотрудников может привести к юридическим и финансовым убыткам, неправильному определению размера выплат.

Затем проводим анализ угроз. В ходе исследования были выявлены следующие актуальные угрозы.

1. Запуск специально разработанных программ, реализующих НСД к ИСПДн. Эти угрозы направлены на выполнение таких действий, как уничтожение, копирование, перемещение, форматирование носителей информации и т. д. Это происходит с использованием стандартных функций операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для этого программных средств, таких как вирус-шифровальщик (троянский конь).

2. Подбор паролей. Злоумышленник может осуществить атаку, применяя различные методы, включая простой перебор, использование специальных словарей или внедрение вредоносного программного обеспечения для перехвата пароля. В случае успеха злоумышленник может установить «заднюю дверь» для последующего доступа. Для смягчения такой угрозы можно увеличить временную сложность процесса подбора пароля, например, увеличив его длину и сложность или ограничив количество неверных попыток ввода пароля за определенный промежуток времени. Эти меры могут быть реализованы через сочетание организационных и технических действий.

3. Нарушения безопасности персональных данных, вызванные ошибками пользователей. Из-за человеческого фактора злоумышленник может добраться до данных. Пользователи могут хранить пароли на бумаге, оставлять их рядом с компьютером или передавать третьим лицам. Кроме того, непреднамеренные действия пользователей могут нарушить целостность, доступность и конфиденциальность персональных данных.

Выше были перечислены актуальные угрозы ПДн для рассматриваемой системы, определены потенциальные нарушители. Перечень актуальных угроз составлен экспертным методом в соответствии с Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн [8].

Таким образом, после оценки эффективности текущих защитных механизмов мы пришли к выводу, что требуется усиление системы защиты путем внедрения дополнительных мер, так как выявлены актуальные угрозы.

Исходя из перечня актуальных угроз, сформированы требования к комплексу мер по защите ПДн.

Первое требование – устранить запуск специально разработанных программ, реализующих НСД к ИСПДн; второе – предотвратить выявление паролей; третье – сократить ошибочные действия пользователей, приводящие к нарушению безопасности персональных данных.

В ходе защиты ИСПДн «Бухгалтерия» следует выбрать средства защиты информации, которые покрывают своими функциональными возможностями весь комплекс предъявляемых мер. Ниже приведена структура комплекса мер защиты (рис. 1 и 2).

Следуя этим требованиям, были выбраны технические средства защиты и разработаны организационные меры, которые полностью удовлетворяют всем требованиям. Мы отдали предпочтение сертифицированным средствам защиты, и в качестве технического решения была выбрана платформа SecretNetStudio.

Рис. 1. Комплекс мер защиты

Рис. 2. Структура комплекса мер защиты ПДн в ИСПДн «Бухгалтерия»

Организационно-распорядительная документация – это набор неотъемлемых документов, который определяет роли, обязанности, цели и права всех работников, включая руководителя и администратора безопасности, в рамках информационной системы по защите персональных данных.

В качестве организационной меры был проведен анализ уже имеющейся политики безопасности ИСПДн «Бухгалтерия», а также ее проверка на соответствие требованиям законодательства Российской Федерации в сфере защиты информации.

Поскольку часть документов политики безопасности не была актуализирована на момент проведения проверки (требовали модернизации и дополнения), было принято решение о внесении изменений в политику обработки и обеспечения безопасности персональных данных в информационной системе «Бухгалтерия», а также в документ, регламентирующий процессы обработки и обеспечения безопасности персональных данных в этой системе, чтобы они полностью соответствовали всем требованиям действующего законодательства Российской Федерации.

Было разработано приложение для сотрудников под названием Security Policy. Основная его цель – упростить процесс знакомства и подписания созданных документов, обеспечивающих безопасность информационной системы по защите персональных данных «Бухгалтерия». После того как пользователь из бухгалтерии вводит свои ФИО, возраст и должность, приложение предоставляет ему перечень необходимых документов. После ознакомления пользователь нажимает кнопку «согласен». Приложение записывает это действие в базу данных, включая ФИО пользователя и информацию о том, ознакомился он с документацией или нет.

Затем проводим повторный анализ угроз по «Методике определения актуальных угроз безопасности» [8]. Результаты повторного анализа приведены на рис. 3, на котором мы можем увидеть, что количество актуальных угроз снизилось до нуля, так как ни одна из угроз не имеет характеристик «возможность реализации» и «опасность» одновременно на втором уровне.

Исходя из повторного анализа угроз, можно сделать вывод, что после внедрения и реализации комплекса мер защиты персональных данных в информационную систему «Бухгалтерия» АО «АИМ» вероятность реализации актуальных угроз стала «низкой». Это означает, что и угрозы перешли в разряд «неактуальных».

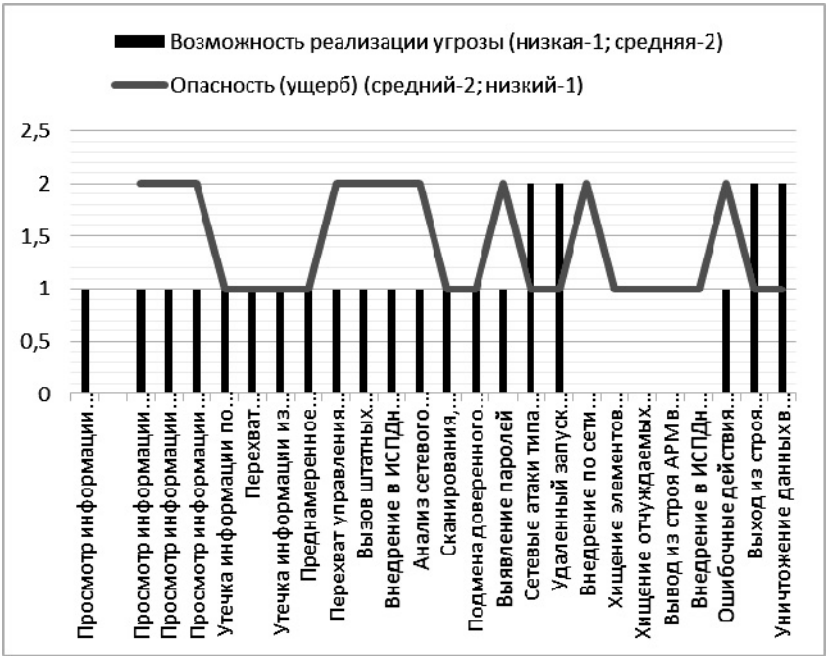

Рис. 3. Повторный анализ угроз

ЗАКЛЮЧЕНИЕ

Таким образом, был проведен анализ нормативно-правовых актов в сфере обработки персональных данных и требований к их защите, оценен исходный уровень безопасности информационной системы персональных данных и имеющихся средств защиты, а также проанализированы существующие актуальные угрозы. На основе этого анализа были выбраны организационные и технические меры защиты информационной системы.

Была выполнена установка и настройка Secret Net Studio. В ходе этой работы произведена актуализация политики безопасности и ее приложений. Дополнительно было разработано клиентское приложение Security Policy.

В результате была успешно выполнена задача по созданию системы защиты для обеспечения безопасности персональных данных в информационной системе предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 30.05.2024).

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 30.05.2024).

3. Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон "О персональных данных"» // КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_117437/ (дата обращения: 30.05.2024).

4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.05.2024).

5. 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» // ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 30.05.2024).

6. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Гарант.Ру: сайт. – URL: https://base.garant.ru/193875 (дата обращения: 30.05.2024).

7. Методический документ ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности информации» // ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 30.05.2024).

8. Методический документ ФСТЭК России от 14.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» // ФСТЭК России – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (дата обращения: 30.05.2024).

9. *Гаврющенко А.П.*, *Масленников А.В.* О методике определения актуальных угроз информационной безопасности с использованием БДУ ФСТЭК // Auditorium. – 2022. – № 2 (34). – С. 37–43.

10. Государственный реестр сертифицированных средств защиты информации // ФСТЭК России – URL: https://reestr.fstec.ru/reg3 (дата обращения: 30.05.2024).

11. Secret Net Studio 8.5. Руководство администратора. Настройка и эксплуатация. – М.: Код безопасности, 2019. – 106 с.

12. Secret Net Studio 8.5. Руководство администратора. Локальная защита. – М.: Код безопасности, 2019. – 159 с.

13. *Исаев А.С., Хлюпина Е.А.* Правовые основы организации защиты персональных данных. – СПб.: НИУ ИТМО, 2014. – 106 с. – URL: https://books.ifmo.ru/file/pdf/1570.pdf (дата обращения: 30.05.2024).

14. *Слепов О.* Защита персональных данных. – URL: https://www.jetinfo.ru/zaschita-personalnykh/ (дата обращения: 30.05.2024).

15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка): (утв. ФСТЭК РФ 15.02.2008) // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_99662 (дата обращения: 30.05.2024).

Карпова Надежда Евгеньевна, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность» Самарского государственного технического университета. Основные направления научных исследований – автоматизированные интеллектуальные системы и автоматизированные информационно-измерительные системы. Имеет более 100 публикаций. E-mail: esib@samgtu.ru

Бабинова Анна Андреевна, ассистент кафедры «Информатика и прикладная математика» Самарского государственного технического университета. E-mail: anyuta.babinova2000@yandex.ru

DOI: 10.17212/2782-2230-2024-2-55-68

Ensuring the security of personal data in the enterprise information system*

N.E. Karpova[1], A.A. Babinova[2]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of technical sciences, associate professor of the electronic systems and information security department. E-mail: esib@samgtu.ru*
[2] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, assistant of the department of Applied Mathematics and Computer Science. E-mail: anyuta.babinova2000@yandex.ru*

With the modern development of information technologies, resources and computerization of society all over the world, in each of the spheres of human activity is not done without information technologies. Some of them are unique and generate income by their uniqueness, and as a result, one of the most urgent problem becomes the provision of information security in any organizations and enterprises, for any sphere and business activities.
Because people want to profit, they can commit criminal acts against the source of income that is always information. The most common source is personal data. In any organization or enterprise there are threats to the security of information that contains personal data. This information may be lost, copied, altered or blocked either by the perpetrator for profit or by mistake or negligence. Loss of confidential information can have both minor and very serious consequences. Therefore, personal data security plays an important role in maintaining and improving the activities of organizations, as it is a problem in all spheres of life.
This article discusses issues related to the development of a system to ensure the security of personal data in the enterprise's information system. During the implementation of the work, the regulatory acts in the field of protection and processing of personal data in the information system of the enterprise were analyzed, the analysis of the existing means of protection and initial protection of IPSDN was made.
As a result of the work, a system for the protection of personal data in IPDS was developed. Technical and organizational measures were selected and the equipment for the security system was validated.

Keywords: Personal data, Confidential information, Personal data information system, Information technologies, Basic security, Actual threats, Intruder, Security measures, Security system

REFERENCES

1. Convention on the Protection of Natural Persons in the Automated Processing of Personal Data (Strasbourg, 28 January 1981). *Konsul'tantPlyus*. (In Russian). Available at: http:///ww.consultant.ru/document/cons_doc_LAW_121499/ (accessed 30.05.2024).

* *Received 20 April 2024.*

2. Federal Law of the Russian Federation of July 27, 2006 No. 152-FZ "About personal data". *Konsul'tantPlyus*. (In Russian). Available at: http:///www.consultant.ru/document/cons_doc_LAW_61801/ (accessed 30.05.2024).

3. Federal Law of the Russian Federation of July 27, 2011. "On amendments to the Federal Law “About Personal Data”". *Konsul'tantPlyus*. (In Russian). Available at: https://www.consultant.ru/document/cons_doc_LAW_117437/ (accessed 30.05.2024).

4. Federal Law of the Russian Federation of July 27, 2006 No. 149-FZ "On information, information technologies and on information protection". *Konsul'tantPlyus*. (In Russian). Available at: http:////ww.consul.tant.ru/document/cons_doc_LAW_61798/ (accessed 30.05.2024).

5. Order of FSTEC of Russia No. 21 dated 18.02.2013 "On approval of the composition and content of organizational and technical measures to ensure security of personal data during their processing in personal data information systems". *FSTEC of Russia*. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed 30.05.2024).

6. Resolution of the Government of the Russian Federation from 15.09.2008 No. 687 "On approval of the Regulation on the features of the processing of personal data carried out without the use of automation means". *Garant.Ru*: web-site. (In Russian). Available at: https://base.garant.ru/193875 (accessed 30.05.2024).

7. Methodological document of the FSTEC of Russia dated February 05, 2021 "Methods of assessment of threats to information security". *FSTEC of Russia*. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed 30.05.2024).

8. Methodological document of the FSTEC of Russia dated February 14, 2008 "Methods of identification of actual threats of security of personal data during their processing in information systems of personal data". *FSTEC of Russia*. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (accessed 30.05.2024).

9. Gavryushchenko A.P., Maslennikov A.V. O metodike opredeleniya aktual'nykh ugroz informatsionnoi bezopasnosti s ispol'zovaniem BDU FSTEK [On the methodology for determining current threats to information security using the FSTEC databas]. *Auditorium*, 2022, no. 2 (34), pp. 37–43. (In Russian).

10. State Register of Certified Means of Information Protection. *FSTEC of Russia*. (In Russian). Available at: https://reestr.fstec.ru/reg3 (accessed 30.05.2024).

11. *Secret Net Studio 8.5. Rukovodstvo administratora. Nastroika i ekspluatatsiya* [Secret Net Studio 8.5. Administrator's manual. Settings and operation]. Moscow, Kod bezopasnosti Publ., 2019. 106 p.

12. *Secret Net Studio 8.5. Rukovodstvo administratora. Lokal'naya zashchita* [Secret Net Studio 8.5. Admin Guide. Local Security]. Moscow, Kod bezopasnosti Publ., 2019. 159 p.

13. Isaev A.S., Khlyupina E.A. *Pravovye osnovy organizatsii zashchity personal'nykh dannykh* [Legal framework for personal data protection organization]. St. Petersburg, ITMO University Publ., 2014. 106 p. Available at: https://books.ifmo.ru/file/pdf/1570.pdf (accessed 30.05.2024).

14. Slepov O. *Zashchita personal'nykh dannykh* [Protection of personal data]. Available at: https://ww.jetinfo.ru/zaschita-personalnykh/ru (accessed 30.05.2024).

15. Basic model of threats to the security of personal data during their processing in personal data information systems (Extract) (approved by the FSTEC of Russia in 15.02.2008). *Konsul'tantPlyus*. (In Russian). Available at: http://www.consultant.ru/document/cons_doc_LAW_99662 (accessed 30.05.2024).

Для цитирования:

Карпова Н.Е., Бабинова А.А. Обеспечение безопасности персональных данных в информационной системе предприятия // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 55–68. – DOI: 10.17212/2782-2230-2024-2-55-68.

For citation:

Karpova N.E., Babinova A.A. Obespechenie bezopasnosti personal'nykh dannykh v informatsionnoi sisteme predpriyatiy [Ensuring the security of personal data in the enterprise information system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 55–68. DOI: 10.17212/2782-2230-2024-2-55-68.