АНАЛИЗ ЭТАПОВ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Бурькова Е. В., канд. пед. наук, доцент, Недорезова А. С.
Оренбургский государственный университет

В современном мире глобальной информатизации, в условиях непрерывного роста киберугроз, защита персональных данных (ПДн), размещенных в информационных системах, становится все более актуальной задачей, привлекающей внимание международного сообщества. На IV Международной конференции «Защита персональных данных», организованной при поддержке Роскомнадзора в ноябре 2017 года, обсуждались насущные проблемы, связанные с персональными данными, были выработаны перспективные предложения и инициативы в сфере регулирования и контроля защиты персональных данных, взаимоприемлемых норм правоприменения законодательных новаций в области защиты персональных данных.

Главной целью создания системы защиты персональных данных объекта информатизации, является предотвращение или сведение к минимуму ущерба (косвенного, материального, морального, вещественного и т. д.). Ущерб возникает в результате реализации угроз безопасности, источниками которых могут быть субъекты информационных отношений с помощью неправомерного и нежелательного воздействия на информацию, ее носители, систему в целом.

Нормативно-правовой базой обеспечения безопасности персональных данных являются руководящие документы Правительства РФ, ФСТЭК и ФСБ, содержащие требования к мероприятиям по защите ПДн:

− Федеральный закон № 152-ФЗ «О персональных данных»;

− Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

− Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

− Приказ ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

− Приказ ФСТЭК России № 17 от 11 февраля 2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности, которые подразделяются на следующие группы:

- законодательные (правовые);

– организационные (административные);
– физические;
– технические (аппаратные и программные).

Защищаемыми ресурсами, в которых находят свое отражение персональные данные объекта информатизации, являются:

– информационные ресурсы;
– средства и система обработки информации;
– аппаратные средства – ЭВМ и составные части (процессоры, мониторы, терминалы, периферийные устройства - принтеры, контроллеры, кабели, линии связи и т.д.);
– программное обеспечение (ПО) – приобретенные программы, исходные, дополнительное системное ПО, загрузочные модули утилиты, диагностические программы и т.д;
– персональные данные, хранимые временно и постоянно, на различных носителях, печатные, электронные, системные процессы и т.д.

Персональные данные должны быть защищены как от преднамеренной, так и незапланированной угрозы. Создание системы защиты персональных данных, приведение процессов обработки и обеспечение безопасности персональных данных в соответствие с положениями и требованиями нормативных документов позволяет минимизировать риски, связанные с утечками ПДн.

Разработка этапов создания системы защиты персональных данных предполагает определение основных операций по анализу обстановки на объекте, выявление актуальных угроз безопасности и формирование направлений по защите ПДн.

Нами был разработан перечень и описание основных этапов создания системы защиты персональных данных на объекте информатизации, который представлен в таблице 1.

Таблица 1- Анализ этапов построения системы защиты ПДн

Наименование этапа	Содержание этапа	Результат
1	2	3
Обследование объекта обработки ПДн	1. Анализ категорий обрабатываемых ПДн; 2. Анализ программно-аппаратных средств ИСПДн; 3. Анализ угроз ПДн; 4. Определение уровня исходной защищенности ИСПДн; 5. Анализ возможного ущерба.	1. Уровень защищенности ИСПДн; 2. Модель угроз; 3. Модель нарушителя; 4. Предварительная оценка возможного ущерба.

Продолжение таблицы 1

1	2	3
Формирование требований к системе защиты ПДн	Формирование требований нормативно-правовых документов на основании выявленного уровня защищенности ИСПДн.	Перечень требований приказов ФСТЭК к уровню защищенности ИСПДн
Анализ существующих средств защиты ПДн на объекте	Анализ всех имеющихся на объекте средств защиты ПДн: организационно-распорядительной документации, физических средств защиты; аппаратно-программных средств защиты ПДн	Список подсистем, не удовлетворяющих требованиям нормативных документов к защите ПДн
Формирование концепции защиты	Определение направлений защиты: по подразделениям; по уязвимостям; по категориям ПДн	1. Выбранное направление защиты. 2. Выбранный способ построения системы защиты. 3. Составление плана мероприятий по управлению системой безопасности ПДн
	Выбор способов защиты: по направлениям защиты; по актуальным угрозам; по экономическим затратам	
	Решение вопросов управления защитой	
Решение основных вопросов обеспечения защиты ПДн	Подготовка документации; Финансовое обеспечение; Подготовка кадров; Закупка и установка аппаратно-программного обеспечения защиты	Организационно-распорядительные документы; Реализация системы защиты ПДн
Анализ эффективности защиты ПДн	Оценка эффективности системы защиты ПДн	Результаты расчета экономической и технической эффективности системы защиты ПДн

Формирование концепции защиты, является важным этапом организации систем безопасности ПДн, в результате, которого определяется выбор направлений и способов защиты ПДн. На рисунке 1 показана схема формирования концепции защиты ПДн.

Направления защиты могут быть определены по отдельным подразделениям, по уязвимым звеньям ИСПДн, а также в зависимости от категорий обра-

батываемых ПДн. Способы защиты чаще всего реализуют по принципу нейтрализации актуальных угроз безопасноти ПДн, но обязательно учитывают экономический критерий в целях реализации наиболее рациональной системы защиты ПДн.

Рисунок 1 – Схема формирования концепции защиты ПДн

Таким образом, сформированная последовательность этапов создания системы защиты ПДн объекта информатизации позволит спланировать и организовать работу по созданию системы защиты ПДн с учетом наиболее важных критериев, что способствует обеспечению высокого уровня безопасности ПДн объекта.

Список литературы

1. Алексашина, М. Н. Защита персональных данных как условие обеспечения безопасности личности / М.Н. Алексашина // Право и безопасность. – 2014. – № 1. – С. 68-73.

2. Бурькова, Е. В. Задача оценки защищенности информационных систем персональных данных / Е. В. Бурькова, // Вестник Чувашского университета. – 2016. – № 1. – С. 112–118.

3. Бурькова, Е. В. Система защиты персональных данных в высшем учебном заведении / Е. В. Бурькова // Интеллект. Инновации. Инвестиции. –2017. – № 7. – С. 69–74.

4. *Назаров, И. Г. Особенности организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных / И. Г. Назаров, Ю. К. Язов, Е. С. Остроухова // Информация и безопасность. - 2009. Т. 12. - № 1 - С. 71-76.*