УДК 004.056.5

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ НОРМАТИВНО-ПРАВОВОГО ПОДХОДА И МАТРИЦЫ СООТВЕТСТВИЯ

Лошадкина Виктория Максимовна, магистрант,
Никитенко Андрей Владимирович, к.п.н., доцент,
Кириллова Елена Борисовна, старший преподаватель,
Ярославский государственный технический университет

METHODOLOGY FOR ASSESSING THE EFFECTIVENESS OF PERSONAL DATA PROTECTION USING THE NORMATIVE-LEGAL APPROACH AND A COMPLIANCE MATRIX

Loshadkina Victoria, master`s student, lvm24122001@mail.ru,
Nikitenko Andrey, Ph.D. in Pedagogy, nikitenkoav@edu.ystu.ru,
Kirillova Elena, senior lecturer, kirilliova.elena@yandex.ru,
Yaroslavl State Technical University, Yaroslavl, Russia

Стремительный рост количества реализованных угроз информационной безопасности и утечки информации свидетельствует о необходимости создания новых подходов и критериев к проектированию, построению и оценке систем информационной безопасности. В статье представлена методика оценки эффективности защиты персональных данных с использованием нормативно-правового подхода и матрицы соответствия. Методика основывается на комплексном подходе для конкретной организации.

Ключевые слова: *информационная безопасность, персональные данные, матрица соответствия, нормативно-правовой подход, оценка эффективности.*

The rapid growth in the number of realized threats to information security and information leaks indicates the need to create new approaches and criteria for design, construction and evaluation of information security systems. The article presents the methodology for assessing the effectiveness of personal data protection using the normative-legal approach and a compliance matrix. The methodology is based on an integrated approach for a specific organization.

Keywords: *information security, personal data, compliance matrix, regulatory approach, performance evaluation.*

Целесообразность данной работы обуславливается постоянной необходимостью построения новых и улучшения старых систем информационной безопасности. По итогам прошлого года в Российской Федерации произошло более 1 миллиарда утечек персональных данных, что заставляет переосмыслить некоторые основные подходы в построении систем информационной безопас-

ности. Утечка информации может привести к серьезным последствиям как для организации, так и для физического лица, включая финансовые потери и ущерб репутации. Стремительный рост количества реализованных угроз свидетельствует о несовершенстве текущего подхода к построению систем безопасности и необходимости создания новых подходов к проектированию, построению и оценке систем информационной безопасности. На первоначальном этапе создания необходимо проанализировать все существующие оценки рисков и угроз персональных данных, чтобы представить новые критерии их оценивания и возможностей самой системы, а ресурсы, затраченные на постройку такой системы, были направлены только на наиболее опасные угрозы.

Разработка методики оценки эффективности защиты персональных данных (*здесь и далее* - ПДн) позволит организациям соответствовать законодательным требованиям и минимизировать риски утечек информации. Методика также полезна для оценки текущих мер безопасности, выявления уязвимостей и разработки рекомендаций по их устранению.

Методика оценки эффективности защиты персональных данных основывается на комплексном подходе для конкретной организации. Первый этап учитывает нормативно-правовые акты в области обеспечения защиты персональных данных: ФЗ №152 «О персональных данных», Постановление Правительства №1119, приказ ФСТЭК №21, приказ ФСБ №378 для уровня защищенности оцениваемой организации [3].

Данный этап включает анализ структур организации, описание процессов и информационных систем, связанных с обработкой ПДн. Также необходимо выявить: какие организационные и технические меры защиты ПДн имеются в организации? Организационные меры предполагают внутренние правила, процедуры и инструкции по защите данных, технические меры охватывают программные решения, такие как антивирусная защита, системы определения вторжений и технологии шифрования [1]. Понимание данных аспектов позволяет оценить насколько активно организация подходит к вопросам защиты ПДн. Необходимо также определить уровень защищенности персональных данных и тип актуальных угроз. Следует отметить, что набор мер может отличаться. Рассмотренный этап играет важную роль в методике, позволяя выявить уязвимости, собрать всю необходимую информацию об организации для дальнейшего построения матрицы соответствия.

Построение матрицы соответствия – второй этап в разработанной методике. На основании выявленных требований из нормативно-правовых актов составляется матрица, в которой все необходимые меры защиты подразделяются на 4 группы:

- Инфраструктура (G1)
- Приложения (G2)
- Эксплуатация (G3)
- Персонал (G4)

Каждая группа наполняется необходимыми мерами защиты персональных данных для конкретной организации. Налаженное взаимодействие между представленными разделениями позволяет создавать надежную систему, способную защищать данные и обеспечивать бесперебойные процессы с ПДн в компании. Данная матрица представлена на рисунке 1.

Вес группы	Нормативное требование	Мера защиты	Вес меры защиты	Соответствие	Эффективность меры на данный момент	Степень несоответствия	Расчет суммы произведений числителя формулы	Расчет знаменателя формулы	Расчет эффективности всей системы
Группа 1 (G1) N-кол-во мер	Требование 1	Мера 1	P_1= G1/N	S_1	$U_1=S_1 * P_1$	$C_1=1- S_1$	$(S_1 * P_1 * U_1)+ \dots (S_m * P_1 * U_m)+$	$P_1*U_m+ \dots$	КЭС=1-Ch/Z
	…						$(S_k * P_2 * U_k)+\dots$	$P_2* U_k+\dots$	
	Требование n	Мера m	P_1= G1/N	S_m	$U_m=S_m * P_1$	$C_m=1- S_m$	$(S_c * P_3 * U_c)+ \dots$	$P_3*U_c+\dots$	
Группа 2 (G2) N-кол-во мер	Требование 1	Мера 1	P_2= G2/N	S_1	$U_1=S_1 * P_1$	$C_1=1- S_1$	$(S_i * P_4 * U_j)=Ch$	$P_4*U_j= Z$	
	…								
	Требование a	Мера k	P_2= G2/N	S_k	$U_k=S_k * P_2$	$C_k=1- S_k$			
Группа 3 (G3) N-кол-во мер	Требование 1	Мера 1	P_3= G3/N	S_1	$U_1=S_1 * P_3$	$C_1=1- S_1$			
	…								
	Требование d	Мера c	P_3= G3/N	S_c	$U_c=S_c * P_3$	$C_c=1- S_c$			
Группа 4 (G4) N-кол-во мер	Требование 1	Мера 1	P_4= G4/N	S_1	$U_1=S_1 * P_1$	$C_1=1- S_1$			
	…								
	Требование h	Мера j	P_1= G1/N	S_j	$U_j=S_j * P_1$	$C_j=1- S_j$			

Рисунок 1. – Матрица соответствия

В представленной матрице каждая группа имеет собственный вес G, где каждая мера обладает одинаковым весовым коэффициентом P.

Также на рисунке присутствует столбец «Соответствие» (S), который определяет соблюдение той или иной меры в конкретной организации. Данная оценка выставляется путем шкалирования, которая представлена в таблице.

Таблица – Шкалирование показателя «Соответствие»

Полностью соответствует	Частично соответствует, требуются доработки	Не соответствует, необходимо значительно доработать	Не соответствует
1	0,6-0,9	0,2-0,5	0-0,1

Данная шкала представляет собой четкое ранжирование, основанное на уровне выполнения установленных стандартов и требований. Опишем подробно каждый показатель в таблице 1.

– Мера полностью соответствует: разработана, внедрена, функционирует в соответствии с установленным требованием, т.е. отсутствуют выявленные нарушения и недостатки. Организация полностью соблюдает правила, установленные нормативно-правовыми актами;

– Мера частично соответствует, требуются доработки. В организации могут быть внедрены значительные меры защиты, но также могут быть и выявленные недостатки, которые требуют внимания. Компания осознает необходимость защиты ПДн, но сталкивается с некоторыми проблемами;

– Мера не соответствует, необходимо значительно доработать. Существенная часть требований не выполняется, либо не внедрены или работают не эффективно, что повышает риск утечек и инцидентов;

– Мера не соответствует. В организации не реализованы требования нормативно-правового акта.

Еще одним важнейшим показателем в матрице является «Эффективность меры на данный момент» (U), который рассчитывается путем умножения показателей «Вес меры защиты» (P) на «Соответствие» (S). Полученный показатель является неотъемлемой частью расчета коэффициента эффективности всей системы (КЭС). Чем ближе показатель к единице, тем ниже риск. Это обусловлено тем, что мера внедрена, но требует доработок. Также приведен показатель «Степень несоответствия» (C), который необходим для дальнейших вычислений.

КЭС показывает насколько эффективно реализованы меры защиты ПДн. Формула для расчета представлена ниже:

$$КЭС = 1 - \frac{\sum(С * P * U)}{\sum(P * U)}$$

Для наглядного расчета формулы в матрице приведены отдельно расчеты числителя и знаменателя КЭС.

Представленная матрица позволяет систематизировать и структурировать процесс оценки защищенности персональных данных для любой конкретной организации, получая количественный показатель [2, с.2]. Также матрица позволяет оптимизировать процесс защиты ПДн и повысить его эффективность.

Полное применение разработанной методики оценки эффективности защиты персональных данных на организации-заказчике представлена на рисунке 2.

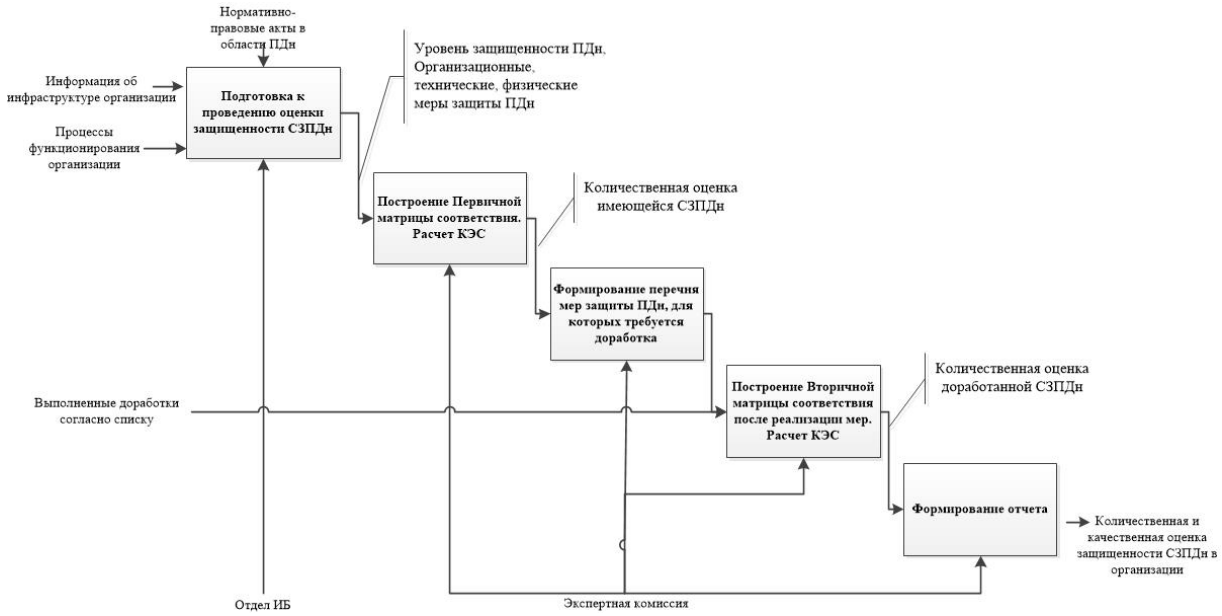

Рисунок 2. – Применение методики оценки эффективности ПДн в организации.

Изначально предоставляются данные об организации, требования и рекомендации из нормативно-правовых актов, на основании которых проводится оценка и исследование. В процессе реализации методики оценки эффективности ПДн необходимо опираться на законность действий, инструкцию и стратегию выполнения методики на основании целей организации.

В результате проведения мероприятий по оценке защиты персональных данных получаются оптимальные показатели минимизации угроз безопасности, а также перечень рекомендаций для оптимизации такой защиты.

Список использованных источников

1. Меркулова, Н.И. Методология моделирования как эффективный инструмент для оценки мероприятий по технической защите персональных данных. [Электронный ресурс].- Режим доступа: https://www.elibrary.ru/item.asp?id=46531689.- Дата доступа 14.03.2025.

2. Шабуров, А.С. Разработка метода оценки эффективности системы защиты информации для коммерческих организаций / А.С. Шабуров, А.И. Шлыков // Вестник ПНИПУ - 2020.- С.2.

3. Приказ ФСТЭК России от 18 февраля 2013 г. N 21. [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya- 2013-g-n-21./ - Дата доступа 12.03.2025.