УДК 004.056

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕТОДИКА ОЦЕНКИ КРИТИЧНОСТИ ИНЦИДЕНТА

О.А. Богушевич, А.С. Гайко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается проблема отсутствия законодательной классификации уровней опасности при утечке персональных данных в Беларуси. Предлагается авторская методика количественной оценки уровня угрозы, базирующаяся на балльной системе с учетом типа данных, масштаба утечки и отягчающих факторов. Разработан алгоритм реагирования для операторов в зависимости от установленного уровня критичности. Обосновывается необходимость принятия специализированного нормативного акта для повышения защиты прав субъектов персональных данных.

Ключевые слова: персональные данные; утечка данных; уровни опасности; защита информации; информационная безопасность; правовая неопределенность; балльная методика; критичность инцидента; алгоритм действий; классификация угроз.

LEAKAGE OF PERSONAL DATA: METHODOLOGY FOR ASSESSING THE CRITICALITY OF AN INCIDENT

O.A. Bogushevich, A.S. Gayko
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article addresses the lack of legally defined danger levels for personal data breaches in Belarus. A methodology for assessing incident criticality is proposed, featuring a scoring system and an action plan for operators. The need for a specialized regulatory act to strengthen the protection of personal data subjects' rights is justified.
Keywords: personal data; data breach; danger levels; data protection; information security; legal uncertainty; scoring methodology; incident criticality; response procedure; threat classification.

Введение

Цифровизация превратила персональные данные в ценный актив, а их утечку – в серьезную угрозу правам граждан. В Беларуси действует Закон «О защите персональных данных», однако он не содержит четких критериев оценки уровня опасности при инцидентах. Это создает правовую неопределенность для операторов и субъектов данных, затрудняя реагирование. Цель работы – анализ текущего регулирования и разработка практического алгоритма действий.

Основная часть

Действующее белорусское законодательство о защите персональных данных базируется на риск-ориентированном подходе. Закон «О защите персональных данных» обязывает операторов принимать меры защиты, соразмерные потенциальному вреду, однако само понятие «вред» и критерии его оценки не детализированы.

Анализ правовых норм позволяет выделить лишь косвенные признаки тяжести утечки: категория данных (обычные, специальные, биометрические), их объем и характер возможного ущерба. Утечка специальных категорий (данные о здоровье, религии, политических убеждениях) несет более высокие риски дискриминации, чем разглашение общедоступной информации. Но единой классификации уровней критичности в настоящее время не существует.

Это создает ряд проблем: у операторов нет ориентиров для реагирования и определения порога уведомления НЦЗПД; возникает субъективизм при расследовании; граждане не понимают серьезности угрозы при компрометации их данных.

Для решения предлагается внедрение балльной методики оценки уровня угрозы. Оператор оценивает три категории: тип утраченных данных (от 1 балла для технических до 10 баллов для специальных), объем

утечки (от 1 балла для 1–10 субъектов до 10 баллов для более 100 000) и отягчающие обстоятельства, которые суммируются. К последним относятся: публикация данных (+3), взлом (+2), отсутствие шифрования (+2), несамостоятельное обнаружение (+1), наличие данных несовершеннолетних или сведений о судимости (+2 за каждый пункт).

Итоговый уровень определяется суммой баллов: 1–5 – низкий, 6–12 – средний, 13–20 – высокий, 21 и более – критический. При утечке специальных категорий данных уровень автоматически признается критическим независимо от иных факторов.

План действий зависит от уровня угрозы. При низком уровне достаточно внутреннего расследования и устранения причин, уведомление НЦЗПД не требуется. При среднем необходимо локализовать инцидент, оценить последствия и рекомендуется уведомить регулятора. При высоком уровне требуется уведомление НЦЗПД в течение 72 часов, оповещение пострадавших и полное расследование. При критическом – уведомление регулятора в течение 24 часов, информирование МВД, публичное заявление и привлечение внешних экспертов.

Данный алгоритм устраняет правовую неопределенность: оператор, получив 15 баллов, понимает, что это высокий уровень, и обязан действовать соответственно – уведомить НЦЗПД в 72 часа и провести расследование, что снижает риски санкций за бездействие.

Заключение

Таким образом, утверждение об отсутствии в Беларуси требований по регуляции уровней опасности при утечке персональных данных является не совсем точным: общие принципы защиты и ответственности закреплены в законе. Однако отсутствие детализированной классификации и четких процедур реагирования на инциденты различной тяжести является существенным пробелом в праве. Предложенный в статье практический алгоритм, основанный на балльной системе оценки и конкретных планах действий, может служить основой для разработки ведомственного нормативного акта НЦЗПД. Внедрение такой методики является необходимым шагом для гармонизации белорусского законодательства с современными вызовами в сфере информационной безопасности и повышения уровня доверия граждан к цифровым сервисам и государственным институтам.

Список использованных источников

1. О защите персональных данных [Электронный ресурс] : Закон Республики Беларусь от 7 мая 2021 г. № 99-З // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=3871&p0=H12100099. – Дата доступа: 15.03.2026.

References

1. On Personal Data Protection [Electronic resource] : Law of the Republic of Belarus dated May 7, 2021 No. 99-Z // National Legal Internet Portal of the Republic of Belarus. – Mode of access: https://pravo.by/document/?guid=3871&p0=H12100099. – Date of access: 15.03.2026.

Сведения об авторах

Богушевич О.А., студент, Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», rebenok1006@gmail.com.

Гайко А.С., студент, Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», sanya040406@gmail.com.

Information about the authors

Bogushevich O.A., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", rebenok1006@gmail.com.

Gayko A.S., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", sanya040406@gmail.com.