СНИЖЕНИЕ РИСКОВ УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПУТЕМ ИХ ОБЕЗЛИЧИВАНИЯ И АНОНИМИЗАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ОБУЧЕНИЯ

Барановский О. К.
Открытое акционерное общество «АГАТ – системы управления» –
управляющая компания холдинга «Геоинформационные системы управления»
Минск, Республика Беларусь
E-mail: baranovskiy-ok@agat.by

Рассмотрен вопрос повышения конфиденциальности пользователей систем электронного обучения в условиях регистрации их цифрового следа. Предложен подход по совместному применению методов обезличивания и анонимизации персональных данных при сохранении возможности их безопасного использования, в том числе для целей повышения качества образовательного процесса.

Введение

Существенный вклад в развитие систем электронного обучения (далее – СЭО) на основе результатов анализа больших данных, представляющих собой цифровой след обучающихся, определяется применением аналитических методов выявления скрытых (изначально неформализованных) закономерностей в сгенерированных массивах образовательных данных. Соответственно, СЭО являются инструментом обработки широкой номенклатуры персональных данных (далее – ПДн) обучающихся. И если перечень ПДн, получаемых от субъекта для целей оказания образовательных услуг, однозначно закрепляется документально до момента их сбора, то согласование с субъектами ПДн полного перечня генерируемых в СЭО ПДн, в том числе с использованием интеллектуального машинного анализа цифрового следа субъектов ПДн, является редкой практикой у операторов ПДн. По мнению экспертов, к недопустимым событиям информационной безопасности в учреждениях образования, эксплуатирующих СЭО, является кража ПДн субъектов образовательного процесса [1]. По сравнению с отказами в обслуживании СЭО, утечка массивов данных с ПДн наносит более высокий ущерб репутации учреждений образования.

I. Цель

Приоритетной задачей при обработке ПДн пользователей СЭО является защита их от утечки с последующей потерей конфиденциальности. В этой связи наряду с выполнением обязательных требований законодательства по защите ПДн от несанкционированного доступа (далее – НСД), оператор ПДн (владелец СЭО) реализует иные меры на соответствие требованиям, которые декларируются законодательством как рекомендуемые [2]. К техническим мерам защиты информации относят реализацию методов обезличивания ПДн в прикладном программном обеспечении. Целью работы является установление подхода по обезличиванию и анонимизации ПДн в СЭО в целях снижения рисков их утечки в результате осуществления НСД к данным в СЭО с их последующей выгрузкой вследствие отсутствия или обхода реализованных мер защиты информации.

II. Подход к обезличиванию и анонимизации персональных данных

Будем учитывать, что законодательство Республики Беларусь определяет обезличивание ПДн как действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн. Это означает, что для обеспечения функционирования систем обработки ПДн применяются средства восстановления (деобезличивания) ПДн. При этом исследователи в сфере информационной безопасности неоднократно доказывали возможность повторной неправомерной персонализации обезличенных ПДн вследствие некорректного применения методов обезличивания.

Законодательством регламентированы методы обезличивания, подлежащие применению в системах защиты информации информационных систем: введение идентификаторов, изменение состава, декомпозиция, перестановка, зашифрование [2]. Методы обезличивания применяются для защиты ПДн при их хранении. Очевидно, что для заданной модели угроз (модели атак) ПДн выбор методов обезличивания и их комбинация будет определяться не менее чем тремя факторами: категориями ПДн (определяют уровень ущерба для субъектов ПДн); информационными технологиями обработки, хранения, передачи и удаления ПДн; показателями производительности основных операций над ПДн, реализующих функции назначения СЭО.

Например, при использовании СУБД выбор и комбинация методов обезличивания будет определяться приоритетами в номенклатуре операций над записями: быстрый поиск, каскадное изменение или удаление, иные сочетания групповых операций, формирование обезличенных или персонализированных выборок. Использование ма-

шинной обработки ПДн всегда предпочтительней ручной обработки администратором или пользователем с высокими привилегиями в СЭО.

Выбор и вычислительная сложность реализации методов обезличивания должны определяться путем обработки рисков, связанных с утечкой ПДн. Экспертами принято, что потеря конфиденциальности ПДн, содержащими сведения об академической успеваемости, оценках и результатах аттестации оценивается как средний уровень ущерба, поскольку ожидается, что в этом случае субъекты ПДн столкнутся со значительными неудобствами [3]. Вместе с тем, данные, накопленные в результате взаимодействия обучающегося с СЭО, (цифровой след) могут содержать сведения, если не явно выявляющие, то позволяющие извлекать информацию о когнитивных, творческих, коммуникативных способностях субъектов, их политических взглядах, религиозных и других убеждениях, а также биометрические поведенческие характеристики. Соответственно, при оценке риска необходимо принимать высокий уровень ущерба.

При формировании перечня ПДн, следует учитывать следующее. Во-первых, СЭО, которые, как правило, строятся на основе проприетарного или свободно распространяемого ПО, ведут запись событий о функционировании ПО и действиях пользователей в журналы. Платформа Moodle журналирует связанные с пользователями события в таблицу базы данных: дата и время события, IP-адрес компьютера пользователя, фамилия, имя и отчество пользователя, действие, выполненное пользователем, название и компонент события, дополнительная информация. Во-вторых, ПДн могут генерироваться при анализе больших данных, выгруженных из СЭО и являющихся цифровым следом при взаимодействии обучающихся со средствами аудио-, видеоконференцсвязи, средствами совместной работы с учебным и справочным материалом в графической и текстовой формах.

Между тем, согласно законодательству [4], содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям их обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки. Соответственно, если цели обработки – оказание образовательных услуг, то повышение их качества или развитие СЭО – это иная цель и должно быть получено согласие обучающегося (он имеет право отказаться) с предоставлением полного списка собираемых ПДн.

Вместе с тем, не требуется получать согласие владельца ПДн, если ПДн обрабатываются на основании законодательства. К подлежащим регистрации содержащих ПДн событиям, связанным с защитой информации и не требующим согласия на их сбор, можно отнести идентификацию и аутентификацию пользователей, нарушение прав доступа пользователей, выявленные нарушения информационной безопасности и др. [2], также для прикладного программного обеспечения: аутентификация (вход и (или) выход) пользователей, успешные и неуспешные попытки аутентификации; неудавшиеся или отмененные действия пользователей; действия пользователей (доступ к объекту (данным), изменения объекта (данных), удаление объекта (данных).

Для целей повышения качества образовательных услуг предпочтительней использовать методы анонимизации ПДн, что предотвратит несанкционированный поиск персонифицированной информации в больших данных (запись в журнале считается анонимной, если ее данные, по отдельности или в сочетании с другими данными, не могут быть связаны с конкретным субъектом ПДн).

В этой связи операторы ПДн (владельцы СЭО) принимают решение о номенклатуре собираемых ПДн для целей оказания образовательных услуг в соответствии с законодательством, а также о номенклатуре ПДн, немедленно анонимизируемых после их получения с дальнейшим их использованием для целей повышения качества образовательных услуг и развития СЭО.

Заключение

Система образования Республики Беларусь находится на этапе, когда проблема обеспечения конфиденциальности обучающихся при использовании СЭО уже замечена, но для ее решения принято недостаточно мер. Учреждения образования с разным темпом вырабатывают практики снижения рисков утечки ПДн при автоматизированной обработке образовательных данных.

1. Positive Research / 2023. Сборник исследований по практической безопасности [Электронный ресурс] – Режим доступа: `https://ptresearch.media/`. – Дата доступа: 26.09.2023.
2. О мерах по реализации Указа Президента Респ. Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 22 февраля 2020 г., № 66 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.
3. Alier, M. Privacy and E-Learning: A Pending Task / M. Alier, M. J. Casan Guerrero, D. Amo, C. Severance, D. Fonseca // Sustainability. – 2021. – Vol. 13. – № 16. – P. 9206.
4. О защите персональных данных [Электронный ресурс] : Закон Республики Беларусь, 7 мая 2021 г., № 99-З // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.