УДК 34

Требования по защите персональных данных при использовании облачных технологий

Рузаев Евгений Павлович
Приамурский государственный университет имени Шолом-Алейхема
Студент

Аннотация
В данной статье определяются основные требования к операторам и облачным провайдерам, которые осуществляют обработку персональных данных. Анализируется законодательство, которым регулируется обработка персональных данных. Выявляются типы угроз, которые возникают при обработке персональных данных в «облаке»
Ключевые слова: персональные данные, идентификация, оператор

Requirements for the protection of personal data when using cloud technologies

Ruzaev Evgeny Pavlovich
Sholom-Aleichem Priamursky State University
Student

Abstract
This article defines the basic requirements for operators and cloud providers who process personal data. The legislation regulating the processing of personal data is analyzed. The types of threats that arise when processing personal data in the cloud are identified
Keywords: personal data, identification, operator

Актуальность темы заключается в том, что высокие темпы информатизации современных технологий повышают риски возникновения уязвимостей в системах информационной безопасности организаций и используются нарушителями для получения несанкционированных персональных данных и интеллектуальной собственности. Для повышения безопасности информации необходимо, чтобы операторы и облачные провайдеры осуществляли свою деятельность строго в соответствии с законом.

Цель данной статьи заключается в определении требований к операторам и облачным провайдерам, которые осуществляют обработку персональных данных в «облаке», а также в изучении законодательства Российской Федерации относительно этого вопроса.

В своей статье А.Г. Абрамова изучает современные проблемы, связанные с защитой персональных данных в Интернете, а также анализирует

основные принципы, используемые в этой области, работа также посвящена методике реализации этих принципов на практике. В данной статье автор рассматривает некоторые особенности передачи персональных данных за пределы государства, их особенности и роль в сохранении конфиденциальности информации, а также основные принципы защиты персональных данных [6]. В работе В.Г. Арбузановой анализируются проблемы информационной безопасности персональных данных, методы оценки угроз персональных данных, приведена классификация угроз персональных данных, представлены основные средства защиты информации в облачных технологиях [7]. Статья А.Л. Гильманшиной направлена на совершенствование системы комплексных мер организационно-правового характера для повышения защищенности информации [8].

В Российской Федерации для обработки информации был принят Федеральный законом от 27.06.2006 № 152— ФЗ «О персональных данных», а также ряд других законодательных актов, к которым относится: Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационно-технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; Приказ ФСБ России № 378 от 10.07.2014 «Об утверждении состава и содержания организационно-технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием криптографических средств защиты информации, необходимых для соответствия требованиям, установленным Правительством Российской Федерации к защите персональных данных для каждого из средств безопасности» [1; 2; 3; 4; 5].

По сути, любые субъекты, которые взаимодействуют с информацией и персональными данными, обязаны соблюдать эти законы, чтобы избежать штрафа от Роскомнадзора. На мой взгляд, компании должны заботиться не только о данных своих клиентов или подрядчиков, но и о сотрудниках. В соответствии с пунктом 1 статьи 3 вышеупомянутого закона, персональными данными является любая информация, относящаяся прямо или косвенно к конкретному или идентифицируемому физическому лицу (субъекту персональных данных) [1].

Все действия с персональными данными и информацией, включая сбор и хранение, называются обработкой информации. Таким образом, обработка — любое действие (операция) или совокупность действий (операций), выполняемых с персональными данными с использованием средств автоматизации или без них, включая сбор, запись, систематизацию, хранение,

накопление, уточнение (обновление, модификация), извлечение, использование, раскрытие (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

То есть, в зависимости от степени использования компьютерных систем при обработке информации она делится на три типа: автоматизированная, смешанная и неавтоматическая. Организация, которая обрабатывает персональные данные, является поставщиком персональных данных.

Под оператором же понимается государственный орган, муниципальный орган власти, юридическое или физическое лицо, которое самостоятельно или совместно с другими лицами организует и/или обрабатывает персональные данные и определяет цели обработки, включая подлежащие обработке персональные данные, действия (операции), которые регистрируются с персональными данными.

В ст. 5 вышеуказанного закона сформированы следующие правила обработки персональных данных, которые должны стать, своего рода, ориентиром для операторов:

1. законность и беспристрастность обработки. Обработка персональных данных должна быть законной и беспристрастной. Если речь идет об обработке данных работника, она должна осуществляться в соответствии с правовыми положениями, применимыми к трудовым отношениям между работодателем и работником;

2. обработка должна осуществляться в конкретных целях. Вы не должны собирать личные данные просто с мыслью, что они понадобятся вам в будущем. Собранные данные должны соответствовать соответствующим целям обработки данных, которые указаны в соглашении об обработке персональных данных. Невозможно объединять базы персональных данных с несовместимыми целями обработки. Если оператор обрабатывает персональные данные для разных целей, они не могут храниться в одной базе данных. Например, компания не может хранить данные клиентов вместе с данными сотрудников;

4. обрабатывать можно только данные, относящиеся к целям обработки. Этот принцип пересекается со вторым: если оператор обрабатывает персональные данные для целей рассылки, он не должен запрашивать у пользователя биометрические данные, если они не необходимы для обработки в других целях;

5. не превышать объем обрабатываемых персональных данных. Объем обрабатываемых данных должен быть адекватным для намеченных целей;

6. точность, адекватность и актуальность персональных данных. Оператор должен обеспечить актуальность и точность данных: Если данные изменились, оператор должен уточнить их или удалить устаревшие данные;

7. срок хранения персональных данных ограничен целями обработки. После достижения целей обработки персональных данных они должны быть удалены, если нет законной причины не делать этого [1].

Соблюдение условий обработки персональных данных является обязательным. В ходе проверки надзорный орган устанавливает, нарушил ли

оператор закон, принимает решение о дальнейших последствиях для нарушителя нормы.

Существует 3 типа актуальных угроз, перечисленных в Постановлении Правительства № 1119:

1. угрозы первого уровня характерны при наличии недокументированных (нераскрытых) возможностей в системном программном обеспечении информационной системы;
2. угрозы второго уровня характерны при наличии недокументированных (нераскрытых) возможностей в прикладном программном обеспечении;
3. угрозы третьего уровня характерны для информационной системы с недокументированными (нераскрытыми) возможностями в системном и прикладном программном обеспечении [3].

Не существует разницы между типами угроз, с которыми обычно сталкиваются операторы. Угрозы первого и второго типа не актуальны для тех операторов, работа которых планируется на лицензионном системном программном обеспечении в защищенной информационной среде, созданной на основе сертифицированных средств защиты информации.

Для большинства негосударственных организаций подходит законодательство об аттестации. Разница заключается в том, что сертификацию должен проводить лицензиат, в то время как организация может проводить оценку эффективности самостоятельно.

В зависимости от выбранного варианта проверки качества защиты персональных данных оператор выбирает средства защиты информации. В процессе сертификации оператор должен использовать заверенные копии, соответствующие уровню безопасности его системы. Если оператор принимает решение об оценке эффективности, он имеет право использовать несертифицированные SPI, но он должен доказать надзорному органу, что они были протестированы и соответствуют требуемым стандартам.

Особого внимания заслуживает криптографическая защита. Если она используется в системе, то вам необходимо использовать SCSI, сертифицированный ФСБ. Это программы или устройства, которые шифруют документы и генерируют электронную подпись.

Таким образом, субъект, обрабатывающий информацию, в том числе, персональные данные, должен придерживаться следующих рекомендаций: детализировать требования к защите персональных данных при использовании облачных технологий и конфиденциальности персональных данных в соглашении с поставщиком облачных услуг; в случае первичного сбора персональных данных проверить местоположение серверов, используемых облачными сервисами для соблюдения требований локализации; для получения согласия субъектов персональных данных на обработку их персональных данных с использованием облачного сервиса. Для того чтобы выявить все риски и разработать план действий по приведению деятельности компании в соответствие с требованиями законодательства о персональных данных, целесообразно провести полный аудит процессов

обработки персональных данных. Нет сомнений, что такой, относительно, новый сектор отношений стоит продолжать изучать, выявлять новые проблемы, предлагать пути их решения, а законодательство должно реформироваться.

Библиографический список

1. О персональных данных: офиц. текст ФЗ № 152-ФЗ от 27.07.2006 г. – СПС КонсультантПлюс.
2. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: офиц. текст Постановление Правительства № 687 от 15.09.2008 г. – СПС Гарант.
3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: офиц. текст Постановление Правительства № 1119 от 01.11.2012 г. – СПС Гарант.
4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: офиц. текст ФСТЭК № 21 от 18.02.2013 г. – СПС Гарант.
5. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности: офиц. текст ФСБ № 378 от 10.07.2014 г. – СПС Гарант.
6. Абрамова А.Г. Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных // Регион и мир. 2020. № 4. С. 21 – 25.
7. Арбузанова В.Г. Безопасность облачных информационных систем // Научные исследования. 2018. № 6 (26). С. 20 – 22.
8. Гильманшина А.Л. Проблемы совершенствования мер защиты персональных данных // Наука через призму времени. 2019. № 9 (30). С. 38–39.