УДК 341(4-672 ЄС)+(477)

РЕГЛАМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЄВРОПЕЙСЬКОГО СОЮЗУ (GDPR) ТА МОЖЛИВІСТЬ ЙОГО ЗАСТОСУВАННЯ НА ТЕРИТОРІЇ УКРАЇНИ

GENERAL DATA PROTECTION REGULATION AND POSSIBILITY TO APPLY IT IN UKRAINE

Овчаренко Я.О.,
магістрант факультету адвокатури
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена початку застосування Регламенту Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (General data protection regulation/Загальний регламент по захисту даних) від 26.04.2016 р. Досліджено понятійний апарат Регламенту, положення про екстратериторіальність його дії. Регламент проаналізовано в контексті можливості його застосування щодо фізичних та юридичних осіб України. Запропоновано основні шляхи адаптації українського законодавства про захист персональних даних до нових стандартів ЄС.
Ключові слова: Регламент ЄС 2016/679, контролер, оператор (процесор), екстратериторіальність, незалежний контролюючий орган.

Статья посвящена началу применения Регламента Европейского Союза о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных (General data protection regulation / Общий регламент о защите данных) от 26.04.2016 г. Исследован понятийный аппарат Регламента, положения об экстратерриториальности его действия. Регламент проанализирован в контексте возможности его применения в отношении физических и юридических л\иц Украины. Предложены основные пути адаптации украинского законодательства о защите персональных данных к новым стандартам ЕС.
Ключевые слова: Регламент ЕС 2016/679, контролер, оператор (процессор), экстратерриториальность, независимый контролирующий орган.

The article is devoted to the adoption of the Regulations EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EU (General Data Protection Regulation). The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.

The article reveals the contents of the extraterritorial principle of the new European rules for the processing of personal data and the way it applies to all companies that process personal data of residents and citizens of the EU regardless of the location of the company.

The article raises the problem of compliance of the standard of protection of personal data in Ukraine with the standards of the European Union. Taking into account the activity of using modern information technologies, the threat of unauthorized automated processing of personal data, on the basis of the analysis above, it can be argued that Ukraine should implement the new European regulation of personal data and apply a new model of their protection. Ukraine is the state that deals with the EU market and communicates directly with personal data of residents of the European Union (in accordance with clause 2 of Article 3 of the GDPR). In any case the adaptation cannot be avoided on the way to a consistent European integration.

The article contains suggestions and ideas to regulate the conceptual apparatus, to create a new mechanism for the regulation of personal data protection in Ukraine, including but not limited to the creation of an independent control authority, the Commissioner for the control of personal data protection, specialists in the protection of personal data at enterprises, institutions, organizations of Ukraine, in accordance with the GDPR.
Key words: GDPR, controller, processor, territorial scope, supervisory authority, administrative fines, personal data protection.

Постановка проблеми. За сучасних умов масштаби збирання та обробки персональних даних надзвичайно зросли. Органи державної влади та юридичні особи приватного права завдяки стрімкому розвитку інформаційних технологій мають можливість здійснювати збір та обробку персональних даних у необмеженій кількості.

Законодавством Європейського Союзу визначається, що захист фізичних осіб під час опрацювання персональних даних є фундаментальним правом.

Статтею 8 (1) Хартії фундаментальних прав Європейського Союзу і статтею 16 (1) Договору про функціонування Європейського Союзу встановлено, що кожна особа має право на захист своїх персональних даних [1–2].

Правові межі для захисту персональних даних у Європейському Союзі встановила Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року «Про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних» (далі – Директива) – документ, який не був обов'язковим, не мав імперативного характеру, а встановлював певні орієнтири, які держави – члени мали закріплювати у своєму законодавстві у такий спосіб, як вони вважали за потрібне [3].

З огляду на явище транскордонних потоків персональних даних нагальною стала потреба не просто у правовому регулюванні захисту персональних даних, а й у дієвому механізмі жорсткого примусу.

Внаслідок цього 26 квітня 2016 року прийнято Регламент Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (General data protection regulation/Загальний регламент по захисту даних) (далі – Регламент, GDPR).

25 травня 2018 року GDPR почав діяти, а його норми на відмінну від положень Директиви мають пряму дію [4].

Виникає питання: «Що це означає безпосередньо для України?».

Насправді актуальність дослідження цього питання зумовлена не тільки процесом євроінтеграції та підписанням Україною Угоди про асоціацію між Україною та ЄС, а переважно тим, що відповідно до Регламенту передача персональних даних за межі Європейського Союзу буде дозволена лише за умови достатнього рівня захисту персональних даних, що забезпечується в країні, в яку здійснюється така передача.

Крім того, відповідно до п. 11 Плану заходів щодо імплементації Угоди про асоціацію між Україною та ЄС, що був затверджений 25 жовтня 2017 року, Україна має удосконалити своє законодавства про захист персональних даних з метою приведення його у відповідність до Регламенту до 25 травня 2018 року [5].

Натепер цього не відбулося, проте впевнено можна говорити, що для того, щоб Україна успішно пройшла шлях євроінтеграції, імплементації положень GDPR в українське законодавство не уникнути.

Дослідження та публікації. Питання захисту персональних даних досліджувало багато українських науковців, найвагомішими є праці О.А. Баранова, К.С. Мельника, С.А. Серьогіна, О.Ю. Базанова, О.В. Кохановської, О.В.Оніщенко, А.В. Пазюк, В.Г. Пилипчук, В.М. Брижко.

Проте вказані дослідження були проведені до прийняття та набуття чинності Регламентом Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних.

Варто наголосити, що питання практичного застосування нових приписів Європейського Союзу у сфері захисту персональних даних відповідно до GDPR залишаються дискусійними та перебувають на початковому етапі пошуку шляхів їх вирішення.

З огляду на це метою статті є дослідження окремих теоретичних та практичних проблем захисту персональних даних, пов'язаних із прийняттям GDPR, визначення ключових правових вимог, які стосуються безпосередньо України та встановлення базових аспектів, необхідних для адаптації українського законодавства до нового законодавства Європейського Союзу у сфері механізму правового регулювання персональних даних.

Основні питання, на які спрямовано дослідження:

1) яким чином правила, встановлені Регламентом ЄС, розповсюджуються на фізичних та юридичних осіб України;

2) які принципові нововведення містить Регламент порівняно із державним регулюванням захисту персональних даних в Україні;

3) які дії на законодавчому рівні варто здійснити для подальшої адаптації положень України про захист персональних даних до законодавства Європейського Союзу.

Виклад основного матеріалу. Проаналізувавши детально положення Регламенту, можна дійти висновку, що, хоча Україна і не є державою-учасницею Європейського Союзу, правила, закріплені GDPR, можуть стосуватися безпосередньо суб'єктів, що належать до її юрисдикції. Оскільки відповідно до ст. 3 Регламенту «Територіальна сфера дії» GDPR має екстратериторіальну дію, то його положення поширюються не лише на держав – членів ЄС, а й на фізичних та юридичних осіб України у конкретних випадках, передбачених Регламентом:

«<…>2. Цей Регламент застосовується до опрацювання персональних даних суб'єктів, які перебувають у Союзі, *контролером* або *оператором*, який має осідок *поза межами Союзу* (не є резидентом держави – учасниці ЄС), якщо опрацювання даних пов'язано з такими факторами: (а) постачанням товарів чи наданням послуг таким суб'єктам даних у Союзі незалежно від того, чи вимагають оплату від таких суб'єктів даних; (б) моніторингом поведінки суб'єктів даних, якщо така поведінка фіксується у межах Союзу <…>» [4].

Отже, хто є контролером та/або оператором (процесором) відповідно до Регламенту?

Згідно із пунктами 7 та 8 ст. 4 Регламенту контролер – це фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; оператор (процесор) – це фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера [4].

Із комплексного аналізу вищевказаних положень випливає, що, крім самих держав – членів ЄС, дія Регламенту поширюється на контролерів та операторів, які вчиняють такі дії:

– мають співробітників у ЄС;

– проводять кампанії, здійснюють дослідження, моніторинг суб'єктів ринку ЄС (електронна комерція, маркетинг тощо);

– здійснюють будь-яку діяльність, спрямовану на ринок ЄС (постачають товари та надають послуги громадянам ЄС на платній та безоплатній основі);

– використовують персональні дані громадян ЄС для здійснення вищевказаної діяльності.

Оскільки в епоху великих даних правовідносини виникають на перетині юрисдикцій, то персональні дані будь-якої особи, зокрема громадянина України, можуть піддаватися обробці суб'єктами господарювання ЄС, США тощо в режимі реального часу і відповідно до правил цих країн. А також фізичні та юридичні особи України, надаючи послуги, що стосуються використання мережі Інтернет, суб'єктам персональних даних з держав – членів Європейського Союзу, можуть оброблювати персональні дані таких осіб.

Отже, фізичні та юридичні особи України підпадатимуть під регулювання GDPR, перебуваючи у статусі контролера або оператора, як це визначено в самому GDPR за умов, вказаних вище.

Далі слід дослідити ключові нововведення GDPR у контексті моделювання їх застосування до контролерів та операторів персональних даних – фізичних та юридичних осіб України.

Для повного євроінтеграційного процесу стандарт захисту персональних даних в Україні повинен відповідати стандартам ЄС.

На час дії Директиви 95/46/ЄС та перед підписанням Угоди про асоціацію України з ЄС було визнано, що механізм регулювання захисту персональних даних в Україні відповідає стандартам ЄС. Проте Регламент, з одного боку, містить подібні до Директиви за змістом положення, а з іншого – закріплює принципово нові.

У Звіті про виконання Угоди про асоціацію між Україною та Європейським Союзом у 2016 році вказано, що відповідно до статті 15 Угоди Сторони домовились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів [6].

Так, Законом України «Про захист персональних даних» повноваження щодо контролю за дотриманням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. У структурі Секретаріату Уповноваженого Верховної Ради України з прав людини функціонує окремий підрозділ з питань захисту персональних даних, серед основних функцій якого – здійснення контролю за дотриманням прав людини у сфері захисту персональних даних, розгляд скарг громадян та вжиття заходів щодо поновлення їхніх прав у сфері захисту персональних даних, перевірка власників персональних даних. Секретаріатом Уповноваженого Верховної Ради України з прав людини постійно здійснюється моніторинг застосування законодавства з питань захисту персональних даних, за результатами якого вживаються необхідні заходи. Зокрема, регулярно проводяться навчальні лекції для професійних та цільових груп з питань практичного застосування положень законодавства у сфері захисту персональних даних. Крім того, створена робоча група, у рамках якої здійснюється напрацювання змін та доповнень до Закону України «Про захист персональних даних» з метою ліквідації законодавчих прогалин, які були виявлені під час застосування цього Закону та гармонізації із законодавством України про доступ до публічної інформації [7].

1. Спочатку варто провести аналогію ***суб'єктів***, зазначених у законодавстві України та у Регламенті ЄС. Основним законом, який регулює питання персональних даних на території України, є Закон України «Про захист персональних даних». Цей Закон регулює правовідносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основних прав і свобод людини і громадянина (зокрема, права на невтручання в особисте життя) у зв'язку з обробкою персональних даних.

Поняття «контролер» та «оператор» (за визначенням GDPR)можнааналогічнозіставитизпоняттями«володілець

персональних даних» та «розпорядник персональних даних» (за визначенням Закону України «Про захист персональних даних»). Зокрема, для контролера і володільця персональних даних ключовим є встановлення мети та засобів (способів) обробки персональних даних, а для оператора та розпорядника персональних даних ключовим є те, що вони є суб'єктами, яким надано право обробляти персональні дані від імені контролера та володільця персональних даних.

2. Наступним кроком є дослідження ***механізму,*** який пропонує застосовувати GDPR, щоб положення не просто були закріплені на папері, а й ефективно діяли.

У всіх державах – членах ЄС та країнах, пов'язаних економічними відносинами з ними, мають бути створені спеціальні державні інститути для контролю за дотриманням прав у сфері захисту персональних даних.

Відповідно до Глави 6 Регламенту кожна держава – учасник повинна створити *незалежний контролюючий орган (Supervisory authority)* для розгляду скарг, застосування санкцій, співробітництва з іншими контролюючими органами щодо захисту персональних даних [4].

Крім того, організаційно-правове та методологічне забезпечення мають здійснювати національні *Уповноважені органи контролю захисту персональних даних,* мають бути незалежними, підпорядкованими закону та підзвітними парламенту.

Саме ці уповноважені органи повинні призначати уже вищезгаданих контролерів.

Кожен контролер (оператор) на підприємствах та в організаціях з чисельністю працівників понад 250 осіб повинен вести облік діяльності з обробки персональних даних.

Крім того, на підприємствах, в організаціях тощо або їх об'єднаннях усіх форм власності має бути призначений *спеціаліст із захисту даних.*

Якщо контролер або оператор є суб'єктом, який передбачений п. 2 ст. 3 Регламенту, перебуває поза межами ЄС, то він повинен призначити письмово представника в Союзі.

Наприклад, у Європейському Союзі функціонують Європейський Омбудсмен, який призначається та звітує перед Європейським парламентом, та Європейський інспектор із захисту даних, який призначається та звітує перед Європейським парламентом і Радою ЄС [8].

Якщо прослідковувати цей процес на рівні держав – членів Європейського союзу, то можна навести й інші приклади:

– Ірландія, Ісландія, Іспанія – Комісія парламенту та Омбудсмен із захисту даних, підзвітний Парламенту;

– Угорщина – Комісар із захисту інформації, який очолює інститут з питань захисту персональних даних та призначається рішенням Парламенту;

– Франція – Національна комісія з інформатики, яка обирається Парламентом; Комісар із захисту персональних даних, який очолює Французьке агентство з питань захисту персональних даних та призначається рішенням Прем'єр-міністра;

– Швеція – Інспекційна рада та Омбудсмен із захисту даних, що підзвітні Парламенту [9].

3. Щоб положення діяли та застосовувалися, потрібно передбачити жорсткий примус та санкції за порушення положень про захист персональних даних. Варто наголосити, що однією із головних відмінностей GDPR від попереднього регулювання є запровадження значних штрафів. Найменша сума штрафу відповідно до ст. 83 Регламенту складає 20 млн євро (4% від валового доходу контролера та/або оператора). Та варто звернути увагу, що у разі виявлення порушення застосуванню підлягає вища сума штрафу [4]. Для порівняння: відповідно до законодавства України у сфері захисту персональних даних максимальна сума штрафу складає 34 тис. грн (ч. 5 ст. 18839 КУпАП).

Виникає питання: «Якщо фізичні та юридичні особи України можуть підпадати під екстериторіальну дію Регламенту, то чи можна притягти такого порушника до відповідальності та накласти санкції, передбачені Регламентом?».

Звісно, в Україні чіткого механізму застосування штрафів відповідно до законодавства ЄС немає. І натепер є не повністю зрозумілим, яким чином до вищевказаної відповідальності можна притягти порушників (фізичних та юридичних осіб) в Україні.

Порушення контролерами/операторами України положень GDPR може призвести до таких можливих наслідків:

1) якщо під час відкриття рахунку для ведення комерційної діяльності в банку ЄС у базі даних буде наявна інформація про порушення фізичною чи юридичною особою України норм GDPR, то рахунок їм не відкриють;

2) наглядовий орган заборонить суб'єкту права ЄС продовжувати потік або передачу даних в Україну, тобто це призведе до розірвання договірних відносин;

3) ті контролери/оператори України, які відповідатимуть положенням Регламенту, будуть конкурентоспроможними на ринку, їм більше довірятимуть користувачі та контрагенти з ЄС.

Отже, Регламент викладений у такий спосіб, щоб не лише здійснити примус щодо порушників, а й створити такі умови, щоб суб'єкт на території ЄС ретельно обирав контрагентів з обробки персональних даних поза територією ЄС.

Наступним кроком після аналізу нових правил Регламенту щодо захисту персональних даних є дослідження проблеми адаптації українського законодавства до безпосередньо GDPR та встановлення базових кроків для наближення українських положень до європейських.

З огляду на активність використання сучасних інформаційних технологій та загрозу несанкціонованої автоматизованої обробки персональних даних на основі проаналізованого вище можна стверджувати, що Україна повинна впроваджувати нові Європейські положення щодо персональних даних та застосовувати нову модель їх захисту. Нехай поки що не як держава – учасник ЄС, а як держава, фізичні та юридичні особи якої здійснюють свою діяльність на ринку ЄС та мають безпосередній контакт із персональними даними громадян Європейського Союзу (відповідно до п. 2 ст. 3 Регламенту). У будь-якому разі на шляху до послідовної євроінтеграції такої адаптації не уникнути.

До базових та невідкладних кроків адаптації можна віднести такі:

1) затвердження та розробка Верховною Радою України відповідно до Регламенту та стандартів ЄС ефективної державної політики щодо захисту персональних даних та здійснення парламентського контролю у цій сфері;

2) запровадження та закріплення інституту Уповноваженого з питань захисту персональних даних, який повинен бути підзвітним Верховній Раді України, основними функціями якого будуть забезпечення нагляду і контролю та удосконалення нормативно-правової бази з питань захисту персональних даних, а також взаємодія з уповноваженими органами ЄС та країн – членів ЄС з питань захисту даних;

3) покладання на центральні органи виконавчої влади функцій, направлених на захист персональних даних, створення спеціальних підрозділів, які могли б діяти у складі Міністерства юстиції;

4) оскільки в Україні функціонує Адміністрація Державної служби спеціального зв'язку та захисту інформації України, то на неї слід покласти функції організації забезпечення технічного захисту персональних даних в Україні;

5) віднесення до компетенції Державного бюро розслідувань України проведення розслідування правопорушень, які стосуються захисту персональних даних;

6) що стосується судової влади, то можна перейняти досвід Великобританії, де діє суд із захисту даних. Також

можливим видається створення окремих судових палат у складі апеляційних судів або створення спеціалізованого суду з питань захисту інформації (даних), де можна розглядати питання не лише захисту персональних даних, а й порушень щодо приватності життя, обігу публічної інформації, діяльності ЗМІ тощо [10];

7) запровадження в органах, установах, закладах, підприємствах та організаціях посад фахівців з питань захисту персональних даних або покладання цих функцій на окремих працівників цих організацій, як того вимагає ст. 37 Регламенту [4].

Отже, варто наголосити на тому, що Регламент Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (General data protection regulation/Загальний регламент по захисту даних) є принципово новим положенням законодавства Європейського союзу щодо захисту персональних даних. На відмінну від попереднього директивного та рекомендованого регулювання цієї сфери GDPR встановлює чіткі та жорсткі правила, запроваджує дієвий механізм, який дозволить практично застосовувати принципи і норми щодо захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних незалежно від їхнього громадянства або місця проживання, забезпечувати дотримання їхніх фундаментальних прав і свобод, зокрема їхнього права на захист персональних даних.

Завдяки підписанню Угоди про асоціацію між Україною та ЄС, активному процесу євроінтеграції та адаптації українського законодавства до законодавства ЄС та відповідно до самого положення Регламенту, зокрема ст. 3, Україна підпадає під дію GDPR у конкретних випадках.

Отже, фізичні та юридичні особи України, що орієнтуються на ринок держав – членів Європейського Союзу, повинні детально проаналізувати, чи підпадають вони під дію положень Регламенту, якщо так – адаптувати свою політику та процес діяльності щодо обробки та збору персональних даних відповідно до GDPR. І якщо сьогодні важко встановити та дослідити, яким саме чином вони (фізичні та юридичні особи України) можуть притягуватися до відповідальності, передбаченої Регламентом, то це не означає, що варто ігнорувати його положення, оскільки у будь-якому разі негативні наслідки настануть. Навіть якщо це буде не штраф, передбачений ст. 83 Регламенту, то наслідком стане неможливість відкрити банківський рахунок в ЄС, послаблення позицій на ринку ЄС, розірвання вартісних контрактів із суб'єктами ЄС (оскільки останні після 25 травня 2018 року вже обирають собі контрагентів, які не мають порушень у сфері захисту персональних даних).

Що стосується проблеми законодавчого врегулювання, то з огляду на принципову новизну багатьох положень та норм GDPR порівняно з регулюванням захисту персональних даних відповідно до українського законодавства про захист персональних даних у цьому разі слід врахувати суттєві зміни до механізму регулювання та захисту персональних даних в Україні. Зокрема, але не виключно, варто посилити парламентський контроль у цій сфері, привести понятійний апарат українського законодавства у відповідність до законодавства Європейського Союзу, запровадити та врегулювати інститут Уповноваженого з питань захисту персональних даних, створити спеціальні підрозділи у складі центральних органів виконавчої влади із повноваженнями щодо захисту персональних даних, створити незалежний контролюючий орган, запровадити жорсткі санкції за порушення захисту персональних даних тощо.

ЛІТЕРАТУРА

1. Хартія фундаментальних прав Європейського Союзу від 07.12.2000 р. // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/go/994_524.

2. Договір про функціонування Європейського Союзу від 07.02.1992 р; 25.03.1957 р. // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/go/994_b06.

3. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/go/994_242.

4. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679.

5. План заходів щодо імплементації Угоди про асоціацію між Україною та ЄС. URL: https://www.kmu.gov.ua/ua/npas/pro-vikonannya-ugodi-pro-asociaciyu-mizh-ukrayinoyu-z-odniyeyi-storoni-ta-yevropejskim-soyuzom-yevropejskim-spivtovaristvom-z-atomnoyi-energiyi-i-yihnimi-derzhavami-chlenami-z-inshoyi-storoni.

6. Звіт про виконання Угоди про асоціацію між Україною та Європейським Союзом в 2016. URL: https://www.kmu.gov.ua/diyalnist/yevropejska-integraciya/vikonannya-ugodi-pro-asociaciyu/zviti-pro-vikonannya-ugodi-pro-asociaciyu.

7. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI / Верховна Рада України. URL: http://zakon.rada.gov.ua/go/2297-17.

8. Брижко В.М. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. 2016. № 3 (18) С. 45.

9. Буайа Ф. Посібник з європейського права у сфері захисту персональних даних: посібник. URL: https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf.

10. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу: навчальний посібник. URL: http://narodna-osvita.com.ua/2453-navchalniy-posbnik-storya-zahistu-nformacyi-v-ukrayin-ta-provdnih-krayinah-svtu-guz-a-m-skachati-chitati-onlayn.html.