Доставка на софтуер - особености и процеси

Тема №3

Технологични ограничения при доставката на софтуер в зависимост от съответната нормативна уредба

Част 2: Доставка на софтуер със специално предназначение. ECCN класификация. Влияние на криптографските функционалности върху възможностите за доставка

Съдържание

1 Въведение

Правилата за експортен контрол и процесите за доставка на софтуер със специално предназначение са критичен регулаторен аспект на доставката на софтуер. Това е сред ключовите ограничения, налагани върху софтуерната индустрия, а наказанията при неспазването им са изключително тежки. Това се дължи на факта, че тези закони произлизат от националната сигурност и ключовите гео-политически процеси. Тези правила носят със себе си редица технологични съображения, които трябва да се познават и от техническите лица, с цел да се предпази организацията от нарушения.

2 Дефиниции

2.1 Какво наричаме "експорт"?

Съгласно законодателството на Европейския съюз и Съединените щати, "експорт" означава не само физическо изпращане на стоки, технологии и софтуер, но и предаването им по електронен път към дестинация извън ЕС или Съединените щати (или други юрисдикции). Експортът важи и за всяко писмено или устно предаване на технология, включително и когато технологията се описва по телефона. Това включва и едно от интересните правила на САЩ, а именно предоставянето на технологии/сорс код на чуждестранни граждани на територията на САЩ (deemed export).

2.2 Какво наричаме "санкции"?

Санкциите налагат ограничения върху конкретни държави, региони, организации и лица по разнообразни дипломатически, криминални, икономически, хуманитарни и свързани с националната сигурност причини. Обхватът на санкциите варира от специфични икономически и финансови мерки до пълни забрани/ембарго.

Електронното предоставяне на услуги зад граница също подлежи на санкционния режим. Това включва финансови транзакции, услуги свързани с поддръжка и предоставяне на облачни услуги. Тоест, ако ние сме компания в САЩ, която предоставя облачна услуга/софтуер, то ако потребител в България достъпи тази услуга/софтуер ние трябва да се съобразим с действащи санкции, ако има такива.

2.3 Какво наричаме "експортен контрол"?

Регулациите относно експорта се прилагат за контролиране на износа, препращането и трансферите на различни стоки, включително военни и комерсиални продукти с двойна употреба. Тези правила съществуват с цел да се решат международни предизвикателства като поддържането на националната сигурност на всяка отделна държава, разпространението на оръжия за масово унищожение (ядрени, биологични, химични) и тероризма, или да се оказва влияние върху поведението на дадена нация, фирма или лице. По този начин се ограничава износа на стоки, които могат да се използват за неоторизирани цели.

Приложимите ограничения се определят в зависимост от обстоятелствата на всяка сделка:

- Какво се предоставя на клиента/бизнес партньора?
- Дали софтуерът или технологията попада под контролирана класификация съгласно приложимите закони за експортен контрол?
- Къде се предоставя продуктът (към каква дестинация се изпраща/предава) и дали дестинацията е обект на забрана или ограничение?
- Кой участва в сделката и дали страните подлежат на търговски санкции?
- Защо клиентът се интересува от нашия продукт и дали крайната употреба на продукта е забранена или изисква експортен лиценз?

Правилата за експортен контрол се налагат от различни държави и международни организации като САЩ, ЕС и ООН. Точно кои са приложимите законодателства зависи от структурата на организацията и нейната дейност. Ще засегнем тази тема по-късно.

Експортния контрол и санкциония режим определя различни нива на изисквания за износа и забрани:

- Изисквания за лиценз за експорт
- Пълна забрана/ембарго (КНДР, Куба, Иран, Сирия, Крим)
- Частично ембарго (забрана за въоръжаване)
- Рестрикции на конкретни индустрии (финанси, енергетика) или типове изделия (военни изделия, изделия с високи нива на криптографски способности)
- Рестрикция на конкретни дейности и крайни употреби (военни нужди, ядрени опити)

3 Значение на експортния контрол

За компанията е от съществено значение да спазва законите за контрол на износа и санкциите, които действат в страните на Европейския съюз, Съединените щати и всички други приложими местни закони. Износът на стоки (включително софтуер и технология) може да бъде забранен или подлежи на изискване за лиценз за износ. Процедурите за експортен контрол определят към кои изделия и технологии се прилагат такива ограничения.

Спазването на изискванията за контрол на износа и санкциите е ключов фактор за успешното функциониране на компанията и получава внимание от висшето ръководство. Целта е да се поддържа висок стандарт на съответствие и да се работи в посока на подобрения, като се осигурява ежедневната оперативна дейност и се предоставя правна консултация на вътрешните партньори на компанията.

Нарушения на законите за контрол на износа могат да доведат до наказателни, граждански или административни искове. Такива правни действия могат да бъдат насочени срещу компанията и/или лицето, нарушило закона, и да доведат до глоба или дори лишаване от свобода. Освен това на служителите на компанията, които нарушават правилата за контрол на износа и санкциите, могат да бъдат наложени дисциплинарни мерки в съответствие с трудовите закони в тяхната страна. Други последствия биха били нарушения на договорни отношения и правилата, дефинирани от използваните лицензи, загуба на репутация, загуба на възможности и пазарни позиции и други.

4 Удостоверение за крайна употреба

Законите и регулациите за контрол на експорта също така включват задължения за уведомяване на компетентните органи за контрол на износа и изисквания за лицензиране на износ, при необходимост, или други ограничения за стоки, които не са контролирани. Това се прилага, ако компанията-износител има информация за критична крайна употреба на тези продукти. Примери за критични крайни употреби включват:

- връзки с оръжия за масово унищожение (ядрени, биологични или химични) или ракети, способни да доставят такива оръжия
- военни крайни употреби в държави, обект на забрана за въоръжаване
- гражданска атомна енергетика в ограничен брой държави

Затова клиентите (крайните потребители), които оперират в критични индустриални сектори или се класифицират като военни, трябва да попълнят удостоверение за крайна употреба/сертификат за краен потребител.

Освен това, може да бъде изисквано удостоверение за крайна употреба и от клиенти в държави, срещу които САЩ и/или ЕС са въвели частично ембарго, санкции или други ограничителни мерки.

Удостоверенията за крайна употреба са образци, предоставени от компетентните органи за контрол на износа и не трябва да бъдат променяни от компанията или крайния потребител.

5 Предотвратяване на нерегламентиран достъп (гео-блокиране)

Гео-блокирането се отнася до практиката на ограничаване или филтриране на достъпа до определен софтуер, съдържание или услуги, в зависимост от местоположението на потребителя. Това може да бъде постигнато с помощта на географски ограничения, които предпазват определени ресурси

или информация от достъп от страни, които са обект на ембарго или имат ограничени отношения с международната общност.

В контекста на контрола на износа и ембаргото, гео-блокирането може да бъде средство за спазване на законите и регулациите за експортен контрол. Компаниите могат да използват гео-блокиране, за да предотвратят непозволения достъп до определени стоки, технологии или услуги от страни или лица, които са обект на ембарго. Този подход помага на компаниите да спазват ограниченията, установени от контролните органи, и да предотвратяват нарушения на закона.

За компаниите, които се занимават с износ на стоки и услуги, е от съществено значение да бъдат информирани и внимателни по отношение на гео-блокирането и как то може да бъде използвано за съответствие с наложеното ембарго. Това изисква редовно обновяване и поддръжка на системите за гео-блокиране, както и сътрудничество с компетентните органи и експерти по експортен контрол, за да се гарантира съответствие с всички приложими закони и регулации.

Съобразяването с ембаргото и използването на гео-блокирането като инструмент за контрол на износа изисква внимателна стратегия и планиране, но е от съществено значение за спазването на международните норми и правила.

6 Четирите ключови въпроса

При определяне на приложимостта (и степента на приложимост) на правилата за експортен контрол следва да се отговори на четири ключови въпроса.

6.1 Какво? (класификация)

Що се отнася до експортния контрол, хардуер и софтуер не се разграничават и ще се отнасяме към тях с обобщеното понятие "изделие". Компанията, която осъществява експорта трябва да познава добре изделието/технологията, които доставя. На база на това те трябва да бъдат класифицирани, с цел да се определят приложимите рестрикции и изисквания за лиценз. Малко по-късно ще разгледаме използвания формален класификатор (секция "Класификацията в детайли").

Един от основните фактори при класифицирането на изделия/технологии са криптографските способности. Интересен е фактът, че контролът на експорта е приложим дори в случаите, когато продукта не инкорпорира криптографските функции и алгоритми директно в кода си. Вместо това продуктът може да използва криптографската функционалност от друг продукт (библиотека) или посредством криптографски интерфейс да използва способностите на операционната система. Такива продукти се наричат "crypto-aware". Консервативна интерпретация на експортния контрол в САЩ би била "Продукт, който е проектиран или модифициран **да използва** криптография за конфиденциалност на данни". Такава интерпретация прави регулациите валидни за огромен набор продукти. Но е важно да отбележим, че това не означава по-рестриктивна класификация или, че ще има ограничения върху доставката.

Законите и регулациите за контрол на износа и санкциите се прилагат за материални изделия, софтуер и технологии. Грубо казано, съществуват три категории за ниво на контрол върху изделията/технологиите

- **Военни изделия/технологии:** изделия/технологии, специално разработени или предназначени за военни цели. Износът на военни стоки почти винаги изисква лиценз за износ.
- **Изделия/технологии с двойна употреба:** изделия/технологии, които могат да бъдат използвани за военни и граждански цели (с двойна употреба), и които са явно изброени в съответните закони за контрол на износ, например Законодателството за износ на САЩ (Export Administration Regulations/EAR) или Приложение I към Регламент (ЕС) № 2021/821 (Регламент за изделията с двойно предназначение на ЕС). Износът на контролирани изделията с двойно предназначение съгласно законодателството на ЕС винаги изисква лиценз за износ.
- **Всички други изделия/технологии:** Всички останали изделия/технологии обикновено не са предмет на ограничения за контрол на износ. Въпреки това могат да съществуват конкретни забрани и изисквания за лицензи за износ за санкционирани или (частично) обект на ембарго страни.

6.2 Къде? (крайна дестинация)

Крайната дестинация е страната или регионът, където нашето изделие/технология:

- ще бъде изпратено физически
- ще бъде изтеглено дигитално
- ще бъде достъпено
- ще бъде споделено, под формата на знание или сорс код (при условията на deemed export)

Важно е да следим за промени в рестрикциите, наложени върху различните региони и да вземем своевременни мерки за съобразяване с тях. Със страни с пълно ембарго не може въобще да се осъществи транзакция на продукта. При частични ограничения трябва внимателно да се проучи естеството на ограниченията и да се съобрази със спецификите на продукта.

6.3 Кой? (участници в транзакцията)

Дори в страни, върху които няма наложени рестрикции има лица и организации, които са санкционирани и съответно има наложена частична или цялостна забрана за експорт с тяхно участие. Съответно се изисква постоянен скрининг на клиенти и партньори и адекватна реакция при попадане на съществуващ клиент/партньор в санкционен списък.

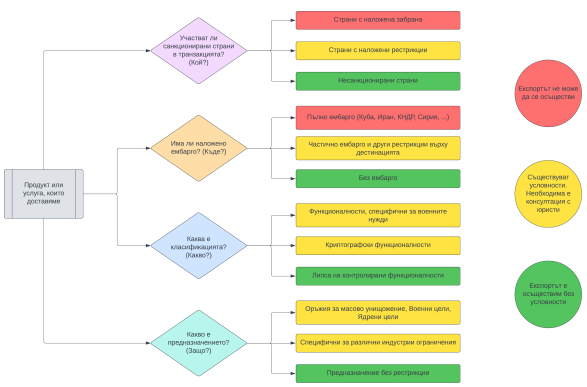
Въпросните санкционни списъци (Sanctioned Party List / SPL) са различни по предназначение и произход. Те уреждат актуалния набор хора, организации и дружества, с които транзакциите са забранени или лимитирани. Те важат и при частична собственост на дадено дружество от санкционирана страна. Забраните/Ограниченията може да са цялостни (софтуер, услуги, финансови транзакции), може само услугите да са позволени, да са за конкретни крайни употреби или с финансов характер.

6.4 Защо? (крайна употреба)

Този въпрос изяснява за какви цели даден клиент има намерение да използва софтуера. На база на това може да се наложат ограничения върху експорта. Примери за употреби, които са забранени или ограничени са:

- Оръжия за масово унищожение (ядрени, биологични, химически) и техните системи за използване (като ракети)
- Военни нужди
- Цивилни ядрени нужди в определени страни
- Конкретни изделия за военни нужди или за военен ползвател в определи страни
- Ограничения в определени сектори - пример е енергийния сектор в Русия и Венецуела

Крайното заключение относно изискванията и възможностите за осъществяване на експорт се базира на комбинацията от четирите въпроса, които показват всички необходими гледни точки, за да се определи това. Основно можем да обобщим взимането на решение със следната диаграма:



Фиг. 1: Взимане на решение относно възможност за експорт

7 Действащо законодателство

Правилата за експортен контрол следват от разнообразна законодателна рамка и набор от регулатори, специфични за конкретна държава или икономически съюз. Сега ще разгледаме САЩ и ЕС като основните страни, от които оперира софтуерния бизнес у нас. Ще обърнем внимание и на други местни регулации за пълнота.

7.1 САЩ

Бюрото по индустрия и сигурност на САЩ (Bureau of Industry and Security / BIS), което е част от Министерство на търговията на САЩ (Department of Commerce), е отговорно за изпълнението и налагането на регулациите за контрол на износа, като въвеждат контрол върху износа и повторния износ на почти всички стоки с двойно предназначение чрез така наречения Export Administration Regulations (EAR). EAR регулира стоки, които се покриват от Списъка за комерсиален контрол (Commerce Control List / CCL). CCL включва 10 категории на стоки и пет групи продукти. Повече детайли малко по-късно в лекцията.

Дирекцията по контрол на търговията с оръжия на Министерство на външните работи на САЩ (Directorate of Defense Trade Controls / DDTC) администрира и налага Регулациите за международния трафик на оръжия (International Traffic in Arms Regulations / ITAR), които въвеждат контроли върху износа, временния внос, повторния износ и прехвърлянето на много военни, отбранителни и разузнавателни стоки (познати още като "стоки за отбрана"), включително свързани технически данни. Списъкът на военни стоки на Съединените щати (United States Munitions List / USML) съдържа стоките, които се регулират чрез Регулациите за международния трафик на оръжия (ITAR), включително гама от продукти от танкове до изтребители. Все пак, отбранителните стоки включват и продукти като сложен военен криптографски софтуер и най-обикновен диагностичен софтуер, предназначен да помага при ремонта на други отбранителни стоки. Освен няколко изключения, CCL включва напълно различен набор от стоки в сравнение с USML.

Офисът за контрол на чуждите активи на САЩ (Office of Foreign Assets Control / OFAC) администрира и налага икономически и търговски санкции въз основа на външнополитическите и свързаните с националната сигурност цели на САЩ срещу определени чуждестранни държави и режими, терористи, международни наркотрафиканти, дейности, свързани с разпространението на оръжия за масово унищожение и други заплахи за националната сигурност, външната политика или икономиката на Съединените щати.

7.2 Европейски съюз

Експортният контрол в Европейския съюз представлява мозайка от правила, установени на равнище на ЕС съгласно законодателството на ЕС и правила, които се прилагат от отделните държави-членки. Тези правила предимно изпълняват експортни контроли върху стоки, уреждани в съответствие с международни рамки, в рамките на които ЕС или неговите държави-членки са страна.

Контролът на износа, относно военни стоки, се урежда от всяка държава-членка на ЕС. ЕС все пак поддържа общ списък на военни стоки, в който са определени такива, подлежащи на контрол при износ. Този списък се приема ежегодно от Съвета, съгласно Общата позиция на Съвета 2008/944/CFSP, уреждаща общите правила за контрол на износа на военна технология и оборудване. Въпреки това този списък няма задължителен характер, и на всяка държава-членка остава да създаде законодателство и въведе свои национални контроли върху износа на военни стоки.

Що се отнася до продуктите с двойно предназначение, регламентът на Съвета (ЕС) 2021/821 (замества Регламент (ЕС) 428/2009) урежда режима на контрол на износа на ЕС, който включва:

- общи правила за контрол на износа, включително общ набор от критерии за оценка и общи видове разрешения (индивидуални, общи и глобални разрешения);
- общ списък на стоките с двойно предназначение на ЕС;
- общи разпоредби за контрол на крайната употреба на непосочени стоки, които могат да се използват, например, във връзка с програми за масово унищожение или за нарушения на правата на човека;

- контроли върху посредничеството и техническата помощ, свързана със стоките с двойно предназначение и транзит през ЕС;
- специфични мерки за контрол и съответствие, които трябва да въведат износителите, като поддържане на регистри;
- разпоредби, установяващи мрежа от компетентни органи, подкрепяща обмена на информация и последователното прилагане и изпълнение на контролите в целия ЕС.

В определени случаи държавите-членки на ЕС могат да въведат допълнителни контроли върху непосочени стоки с двойно предназначение поради обществена сигурност или съображения, свързани с правата на човека.

Стоките с двойно предназначение могат да се търгуват свободно в рамките на ЕС, с изключение на някои особено чувствителни стоки, чието прехвърляне в рамките на ЕС остава подлежащо на предварително разрешение (Приложение IV на Регламента). Регламентът допринася за целите на Общността за атомна енергия на Европейската атомна енергийна общност (Евратом) относно търговията с ядрени материали и мирната употреба на ядрената енергия.

Регламентът се прилага директно в целия ЕС. Въпреки това държавите-членки на ЕС трябва да предприемат национални мерки за прилагане на някои от неговите разпоредби, като например санкции и наказания.

Ограничителните мерки или санкции са важен инструмент на Общата външна политика и политиката за сигурност (ОВППС) на Европейския съюз. Те се използват от Европейския съюз като част от интегриран и всестранен подход към политиката, включващ политически диалог, допълнителни усилия и използване на други инструменти. Ключови цели при въвеждането на санкции включват: защита на стойностите, основните интереси и сигурността на ЕС, запазване на мира, укрепване и подкрепа на демокрацията, правовата държава, правата на човека и принципите на международното право, предотвратяване на конфликти и засилване на международната сигурност.

7.3 Други

Освен тези огромни играчи в световния софтуерен бизнес, има и други правила, с които е възможно фирмите да трябва да се съобразят. Особено за интернационалните компании и компаниите, базирани в по-специфични юрисдикции. Изясняването на въпроса за приложимите правила за експортен контрол ще засегнем малко по-късно.

В Германия Федералният офис за икономика и контрол на износа (Bundesamt für Wirtschaft und Ausfuhrkontrolle – BAFA) е отговорен за предоставянето на необходимите лицензи за износ. BAFA е орган, подчинен на Федералното министерство за икономика и енергетика на Германия (Bundesministerium für Wirtschaft und Energie – BMWi). BAFA е упълномощен да вземе окончателното решение дали стоките от Германия се допускат за износ.

В България Междуведомствената комисия за експортен контрол и неразпространение на оръжията за масово унищожение към Министерство на Икономиката отговаря за прилагането и изпълнението на законодателството (Закон за експортния контрол на продукти, свързани с отбраната, и на изделия и технологии с двойна употреба).

Интересен факт е, че в основата на много от националните режими е Споразумението от Васенаар. Споразумението от Васенаар относно контрола на износа на конвенционални оръжия и стоки и технологии с двойна употреба е едно от многобройните мултилатерални споразумения за контрол на износа, които се съсредоточават върху конвенционалните оръжия и стоки и технологии с двойна употреба.

Споразумението от Васенаар влиза в сила през 1996 г. и има за цел да насърчи прозрачността и по-голямата отговорност при прехвърлянето на конвенционални оръжия и стоки и технологии с двойна употреба, с цел предотвратяване на "дестабилизиращи натрупвания". Към 2023 година в него участват 41 държави, включително Германия и Съединените щати, които, чрез своите национални политики, се стремят да гарантират, че прехвърлянето на тези стоки не допринася за развитието или подобряването на военни възможности, които подкопават тези цели и не се отклоняват да подпомагат такива възможности.

Участващите държави са се съгласили относно списъците с контролирани стоки с двойна употреба и боеприпаси и са отговорни за изпълнението на национални контроли на износа, съобразно списъците и насоките на Споразумението от Васенаар. От особено значение за софтуерния сектор е "Списък на стоки с двойна употреба и списък на боеприпаси" и съответни раздели:

- Категория 5, част 2, отнасяща се до софтуер и криптиране
- Общата бележка за софтуер
- Списъкът с боеприпаси, раздел ML21

Важно е да се отбележи, че почти винаги регулациите около експортния контрол са обвързани с изисквания за внимателно управление и проследимост на всички дейности, които компаниите извършват по отношение на съответствието. Тоест, изисква се поддържането на необходимата документация, отразяваща действията и решенията, която да може да бъде предоставена на регулаторите при поискване.

8 Валидност на правилата за експортен контрол

Валидността на правилата за експортен контрол изглежда на пръв поглед лесна задача за определяне. Валидните правила са тези на страната, от която оперираме - тоест, от която осъществяваме експорта. Например ако компанията ми е базирана в България, то правилата за експортен контрол са валидните за произведения от моята компания софтуер, а експортният режим на Китай е напълно нерелевантен.

Разбира се, ако държавата е част от някаква друга организация, която има регламент за експортен контрол, то този регламент също е валиден. Европейския съюз има такъв. Съответно в България като държава-членка също важи и регламента на ЕС, съответно е валиден и за нашата компания.

Нещата обаче са малко по-сложни.

Една основна трудност са интернационалните компании. Множество големи компании имат подразделения в много точки от света. Екипи от различни местоположения могат да работят заедно, за да създадат един софтуерен продукт. Тогава този продукт с кое законодателство се съобразява? Основно може да се каже, че експорта се осъществява от едно конкретно подразделение, от името на което се участва във всяка транзакция. Седалището на това подразделение определя валидните регулации. Ако множество подразделения осъществяват доставка на софтуерни продукти, то съответните продукти подлежат на регулацията на държавата, в която е регистрирано подразделението.

Това обаче не изчерпва темата. Участието в чуждестранните финансовите пазари, използването на компоненти с произход други страни, осъществяването на сериозен контрол над дейността на фирмата от граждани на други страни и други фактори **могат** да доведат до нуждата да се съобрази доставката с допълнителни режими за контрол на експорта. Важно е да наблегнем на думата "могат", тъй като не е напълно задължително това да е факт и следва да се потърси юридическа помощ, за да се определи.

Особено интересна е ситуацията със законите в САЩ и тяхната приложимост за компании, които са извън САЩ.

EAR разграничава между "износ," "повторен износ" и "публикуване". Износ означава фактическото изпращане или предаване на стоки извън САЩ. Повторен износ означава фактическото изпращане или предаване на стоки, подпадащи под EAR, от една чужда страна, към друга чужда страна. Публикуване (гореспоменатият deemed export) означава предоставянето на технология или софтуер с произход САЩ на лице, което не е гражданин на САЩ, на територията на САЩ. Също съществува и терминът deemed re-export, който е като deemed export, но публикуването се извършва извън САЩ и на лице, което не е гражданин на страната, в която се извършва. При тези случаи, регулациите на САЩ са приложими и е възможно изискване за лиценз. Повторният износ и deemed re-export са от основен интерес в тази секция, тъй като те именно са фактори, които биха направили правилата на САЩ приложими за неамериканска компания.

Компаниите не могат да предполагат, че разрешеният износ на стоки от САЩ означава, че тези стоки могат да бъдат повторно изнесени в трета страна без допълнително разглеждане на законите за контрол на износа от САЩ. EAR изисква износът и повторния износ на стоките да бъдат оценени поотделно. Същите изисквания за лицензиране важат както за повторните износи, така и за износите, тъй като законите за контрол на износа в САЩ регулират продукти с произход от САЩ, независимо къде се намират.

Пример: Германска компания закупува множество копия на софтуерен продукт от американска компания. Американският продавач определи, че продукта подлежи на EAR, но няма нужда от лиценз за износ в Германия, базиран на CCL и Commerce Country Chart, което е таблица в

EAR, включваща всички държави. Сега германската компания планира да продаде копия от този софтуер на клиент в Бразилия, което от гледна точка на EAR би бил повторен износ. Въпреки че не беше необходим лиценз за първоначалния износ в Германия, германската компания ще се нуждае от лиценз от BIS за повторния износ в Бразилия, тъй като изискванията за лицензиране за износа на този продукт са различни за Германия и Бразилия.

EAR може също да се прилага към компании извън САЩ, които произвеждат стоки, съдържащи компоненти или технологии от САЩ. EAR определя прагове "де минимис" въз основа на стойността на компонентите или технологиите от САЩ, вградени в продукт, произведен извън САЩ, за да се определи дали продуктът подлежи на EAR. Правилата за праговете се прилагат в случай на:

1. "вграждане" на контролирани стоки от САЩ в продукт, произведен извън САЩ, или "свързване" с контролиран софтуер от САЩ,
2. "вграждане" на контролиран софтуер от САЩ в софтуер, произведен извън САЩ,
3. смесване на технология, произведена извън САЩ, с контролирана технология от САЩ.

За повечето дестинации и продукти, продукт или софтуер, произведени извън САЩ, подлежи на EAR, ако стойността на контролираното съдържание от САЩ надвишава 25% от общата стойност на завършения продукт. За някои дестинации (например Иран, Сирия), прагът "де минимис" е 10%. Прилагането на прага зависи от ECCN на контролираното съдържание от САЩ и окончателната дестинация, към която се изнася продуктът, произведен извън САЩ. Специални правила се прилагат за високопроизводителни компютри и софтуер за криптография, които биха могли да свалят прага на 0%. Няма праг "де минимис" за продукти, услуги и съответни технически данни за отбрана съгласно ITAR. Веднага когато в непроизведения извън САЩ продукт е внедрен един компонент, подпадащ под ITAR, се прилага ITAR.

Пример: Френска компания закупува софтуер, предназначен за управление на определен вид машини от американска компания. Американският продавач определи, че въпреки че софтуерът е предмет на EAR, няма нужда от лиценз за износ до Франция. Френската компания иска да използва софтуера с произход от САЩ със своя собствена хардуер и да продава свързаните продукти на компания, базирана в Хаити ("свързан" означава, че софтуерът, който се изнася заедно с продукта, е конфигуриран за продукта, но не е физически интегриран в него). Ако стойността на софтуера надвишава 25% от стойността на свързания продукт, френската компания ще се нуждае от лиценз от BIS, преди да може законно да изнесе продукта, защото изискванията за лицензиране на износа за този софтуер са различни за Франция и Хаити.

9 Червени флагове

Във всички сделки с клиенти и потенциални клиенти, винаги организациите трябва да са нащрек за възможни нарушения на разпоредбите, свързани с експортния контрол. Конкретно, посочените по-долу "Червени флагове" или предупреждения указват на риск, че трансмисията на софтуер може да бъде пренасочена към неразрешено местоназначение, потребител или цел, или че продуктите и услугите на фирмата могат да бъдат използвани в забранени дестинации или да бъдат достъпни от там. Някои от тези "Червени флагове" изискват задълбочено познание на клиента, техните организационни структури и техния бизнес. Затова е важно да открием критични факти, които да ни помогнат да се съобразим с разпоредбите. Дори липсваща информация, която не е предоставена от клиента, може да бъде индикация за критична ситуация.

Някои примери за "червени флагове" са:

- Ако сте осведомени, че клиент има или планира да създаде дъщерно дружество, офис, филиал или друг вид оперативно присъствие в забранена държава/регион или провежда бизнес в забранена държава.
- Ако сте осведомени, че клиент споменава продукт(и) на фирмата във връзка с забранена държава/регион (например, се позовава на опит с продукта в Иран).
- Ако сте осведомени, че софтуерът на фирмата или техника на фирмата се използва в забранени държави/региони.
- Ако сте осведомени, че клиент използва методи за преодоляване на IP ограниченията.

- Ако сте осведомени, че броят на лицензите не съответства на бизнеса на клиента (размер и сектор).
- Ако сте осведомени, че крайното използване на продукт не е съобразено с нормалното му използване или е потенциално критично (например, атомни или оръжейни цели и др.).
- Ако сте осведомени, че клиент не желае да предостави информация за крайното използване или крайния потребител.
- Ако сте осведомени, че клиент има малко или никакъв бизнес опит. Например, финансова информация не може да бъде намерена от обичайни комерсиални източници, а собствениците на компанията са непознати за търговските източници.

Всякакви съмнения относно такива клиенти или потенциални клиенти следва да бъдат проучени внимателно и да се вземат необходимите мерки. Всички "Червени флагове" трябва да бъдат разяснени, преди да може да продължи сделката.

10 Класификацията в детайли

Класификацията е основен фактор за определяне на нуждите от лиценз и съответствието с експортния контрол. Ще се фокусираме върху продуктите с двойна употреба, тъй като най-често софтуерните продукти попадат под тях.

При класификацията се използват специални идентификатори, които определят, че дадения продукт попада в съответните списъци (CCL за САЩ и Приложение 1 на Регламент (ЕС) 2021/821 за ЕС). Самите списъци сами по себе си описват конкретни или абстрактни (на база характеристики) продукти. На база на това, ако даден продукт е точно упоменат в списъка или отговаря напълно на упоменати критерии, то той се класифицира със съответния идентификатор. На база на това ще може да се заключи и необходим ли е лиценз за експорта на такива продукти. Самите списъци са сходно структурирани и имат сериозно препокриване (до голяма степен списъка на ЕС е подмножество на този на САЩ). Това е така, защото са базирани на едни и същи международни договори като Споразумението от Васенаар. Въпреки това не е гарантирано, че иден продукт ще получи еднакъв идентификатор спрямо и двата регламента.

При EAR този идентификатор си има име - ECCN (Export Control Classification Number). В Европа си няма, но тъй като често компаниите класифицират и по двата регламента, те използват термина ECCN и за Европа.

Структурата на идентификатора се състои от комбинация от букви и цифри и включва следните елементи:

- **Категория:** Първата цифра определя категорията на продукта или технологията. Например, категория 3 се отнася за "Electronics"
- **Подкатегория:** Следващите цифри уточняват подкатегорията в рамките на основната категория. Например, подкатегория D се отнася за "Software"
- **Контролен номер:** Този номер обикновено съдържа букви и цифри и уточнява конкретния продукт или технология в рамките на подкатегорията.
- **Суфикс:** Формално не е част от идентификатора, но практически е неизменна част тъй като определя приложимите под-точки на дадения идентификатор за продукта. Тези конкретни под-точки често са от значение при взимане на решения.

Като пример, идентификатора 3A225 се отнася до честотни преобразователи, а пък 5A002.a е елемент, който има "информационна сигурност" като основна функция.

10.1 Категории

Възможните категории са следните:

- Категория 0: Ядрени материали, оръжие и специални материали
- Категория 1: Материали, химикали, микроорганизми и токсини (САЩ) / Специални материали и свързано оборудване (ЕС)

- Категория 2: Обработка на материали
- Категория 3: Електроника
- Категория 4: Компютърна техника
- Категория 5: Телекомуникации (част 1) и информационна сигурност (част 2)
- Категория 6: Сензори и лазери
- Категория 7: Навигационно и авиационно оборудване
- Категория 8: Морско оборудване
- Категория 9: Космически апарати и силови установки (двигателни системи)

10.2 Подкатегории

Възможните подкатегории са следните:

- A. Крайни изделия, оборудване, аксесоари, прикачени части, компоненти и системи
- B. Оборудване за тестове, инспекция и производство
- C. Материали
- D. Софтуер
- E. Технология

Продуктите на софтуерната индустрия най-често попадат в категория 5, част 2, подкатегория D поради криптографските си възможности (идентификатор 5Dxxx).

10.3 Изключението ENC в САЩ

Основното изключение за лиценз, което се използва за елементи от категория 5, част 2, е изключението за лиценз ENC. Изключението за лиценз ENC предоставя широк набор от разрешения за продукти за криптиране (елементи, които използват криптография), които варират в зависимост от елемента, крайния потребител, крайното използване и дестинацията. Няма невъзможно ниво на криптиране според изключението за лиценз ENC. Повечето продукти за криптиране могат да бъдат експортирани към повечето дестинации посредством изключението за лиценз ENC, след като износителят е спазил приложимите изисквания за докладване и класификация. Някои елементи, изпращани до определени дестинации, изискват лицензи.

10.4 "Mass market" в САЩ

Хардуерни и софтуерни елементи, които в противен случай биха били класифицирани като 5A002 или 5D002, могат да бъдат класифицирани като 5A992.c и 5D992.c, ако отговарят на критериите, изброени в Забележка 3 към Категория 5, Част 2 ("критериите за масов пазар"). По друг начин казано, някои елементи 5x002 могат да станат 5x992.c в зависимост от начина, по който се продават. Характеристиките могат да бъдат обобщени като:

- Продуктът е общодостъпен за обществото чрез продажба, без ограничение, от складове в търговски обекти чрез следните методи:

  Сделки без предварително съгласие;

  Сделки по пощата;

  Електронни сделки (например, чрез интернет); или

  Сделки по телефон.

- Криптографската функционалност не може лесно да бъде променяна от потребителя;
- Проектът е проектиран за инсталиране от потребителя без по-нататъшна значителна подкрепа от доставчика;

- Когато е необходимо, данни за елементите са достъпни и ще бъдат предоставени по заявка на съответния орган в страната на износителя, за да се установи съответствие с условията.

Въпреки че елементи с ECCN 5A992.c и 5D992.c не изисквта изключение от лиценз, за да бъдат изпратени на повечето места (защото са само контролирани срещу тероризма), те се описват в Изключение от лиценз за криптиране ENC, което включва изискванията за уведомления, които трябва да бъдат направени пред BIS.

10.5 Ако продуктът не попада в списъка

В ЕС, ако елементът се съдържа в Приложение I, то се изисква разрешение за износ / лиценз. Ако елементът не е в списъка, тогава обикновено не се контролира. (Регламентът на ЕС предвижда, че дори тези елементи изискват лиценз, ако са предназначени за използване в програми за масово унищожение или нарушения на правата на човека - обичайно наречени catch-all клаузи).

Системата в САЩ не е толкова ясна - просто защото нещо не е в Контролния списък за стоки не означава, че не се контролира. То все още може да бъде класифицирано като **EAR99** (ако продуктът попада под юрисдикцията на Министерството на търговията на САЩ) и може да изисква лиценз в зависимост от мястото, до кого или за каква цел се изнася.

11 Софтуер с отворен код

Общата бележка за софтуер на ЕС (General Software Note/GSN) в Приложение 1 на Регламент (ЕС) 2021/821 изключва софтуер, който е "в обществения домейн" от това, което трябва да подлежи на експортни ограничения, и актуализираният общ контролен списък на стоките с двойно предназначение на ЕС пояснява, че "в обществения домейн" се отнася до софтуер, който е достъпен без ограничения по отношение на неговото следващо разпространение и, че авторските ограничения в този контекст не премахват софтуера от обществения домейн. Това води до заключението, че за регулациите на ЕС всеки софтуер с отворен код е освободен от експортен контрол, независимо от неговата цел.

Според ръководството публикувано от BIS, промените в правилата от 29 март 2021 г. премахват изискването за изпращане на известие по имейл за криптографския изходен код и бета версиите на криптографски софтуер, достъпни "публично", с изключение на софтуер, който изпълнява "нестандартна криптография", дефинирана като всяка реализация на "криптография", включваща или използваща собствена или непубликувана криптографска функционалност, включително алгоритми или протоколи за криптиране, които не са били приети или одобрени от признати международни стандартизационни организации (например, IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA и GSMA) и не са били публикувани по друг начин. При изпълнение на гореспоменатите условия, софтуера се счита за "публикуван" и не подлежи на EAR.

12 Връзка с каналите за доставка

Както вече знаем, каналите за доставка имат за цел да създадат ясна и повторима процедура за доставка на софтуер при определени условия. Основна задача е да се подсигурят множество изисквания и ограничения, така че извършването на доставката да не противоречи със национални и международни закони и бизнес интересите на фирмата. Именно едно от нещата, които се съблюдават посредством каналите за доставка е съответствието с експортния контрол. Именно канала за доставка може да дефинира правила и процеси, които да ни предпазят от неправомерна доставка. Това може да стане посредством изисквания, които да бъдат проверявани преди всяка доставка, използвани технически средства за предоставяне на достъп, които да имат необходимите възможности за ограничения на употребата и други. В зависимост от типа софтуер, който даден канал цели да доставя, под каква форма е този софтуер, по какъв начин се осъществява достъпа до този софтуер и от кого се достъпва, ние може да дефинираме серия от правила като част от канала за доставка и проверките за възможност за доставка.

13 Заключение

Експортният контрол е изключително важна регулация, несъответствието с която може да доведе до много сериозни последици. За това е много важно внимателно да се осигури съответствието

с нея. От основно значение е доброто познаване на продукта и реципиента му, включително намеренията как ще го използва. На база на това, различните държави и организации имат различни (но не драстично различни) регламенти и изисквания. Масовият софтуер основно попада под регулацията поради криптографските си възможности. Това прави регулацията широко приложима в цялата софтуерна индустрия, налагайки разглеждането и в курса.