European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

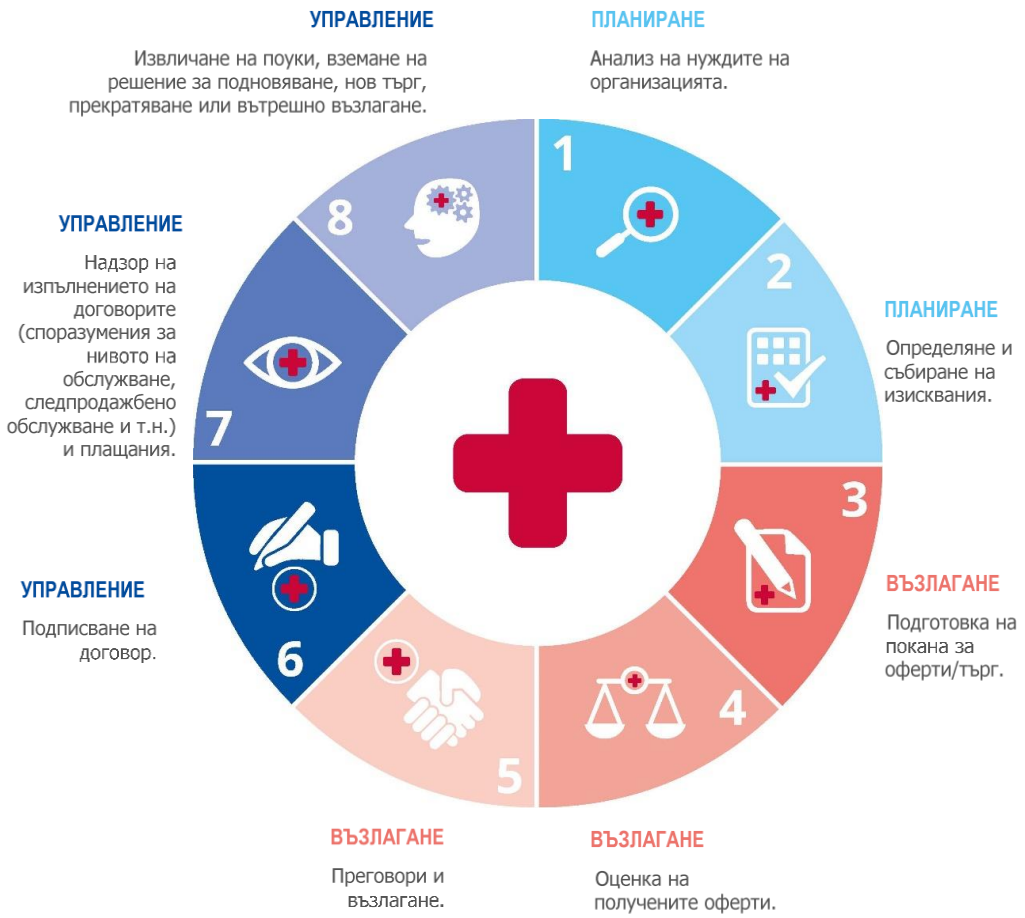
НАСОКИ ЗА КИБЕРСИГУРНОСТ ПРИ ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНИ ПОРЪЧКИ В БОЛНИЦИТЕ

Целта на доклада е да служи като наръчник за медицинските специалисти. Много от практиките и препоръките ще бъдат полезни и за други здравни организации, тъй като процедурите за възлагане на обществени поръчки често са много сходни. Документът е полезен за лица, работещи в здравеопазването, които заемат технически длъжности в болници, т.е. ръководни кадри: главен служител по информацията, главен служител по сигурността на информационните системи, главен служител по техническите въпроси, ИКТ екипи, както и служители в областта на обществените поръчки в здравни организации. В настоящия кратък документ са обсъдени основните елементи на доклада — за повече подробности читателят трябва да се запознае с публикацията на ENISA: ENISA Good Practices for the Security of Healthcare Services („Добри практики на ENSA в областта на сигурността в здравните услуги“), публикуван през февруари 2020 г.

ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНИ ПОРЪЧКИ

Тъй като болничната екосистема съдържа няколко ИТ компонента, киберсигурността следва да се разглежда поотделно във всеки един от тях. Тя следва да бъде част от всички отделни етапи на процедурата за възлагане на обществени поръчки. В този раздел са представени обичайните етапи на процедурата за възлагане на обществени поръчки за снабдяване с продукти и услуги, включително медицински изделия, информационни системи и инфраструктура.

Фигура 1: Жизнен цикъл на процедурата за възлагане на обществени поръчки за болници



- Етап на планиране: Най-напред болницата извършва анализ на нуждите и събира искания от няколко отделения в рамките на вътрешна процедура. Например, при придобиване на нова облачна услуга, ръководният служител по техническите въпроси следва да определи нуждите и да анализира какви ползи предлага използването ѝ.

- Етап на възлагане: След това изискванията се оформят в техническа спецификация и в сътрудничество със службата за обществени поръчки започва процедурата по възлагане (напр. публикува се обява за търг). Болницата получава съответните оферти, комисията (включително главният служител по техническите въпроси/главният служител по сигурността на информационните системи и/или член на ИКТ екипа) оценява офертите и избира най-подходящите продукти. Провеждат се преговори с изпълнителя и се сключва договор.

- Етап на управление: Накрая договорът (в частта по управление и наблюдение на изпълнението) се възлага на служител на болницата, определен като „собственик“. Определеният служител отговаря за приключването на тръжната процедура и за получаването на обратна информация от потребителите относно реалното функциониране на оборудването/системата/услугата.

ВИДОВЕ ОБЩЕСТВЕНИ ПОРЪЧКИ В БОЛНИЦИТЕ

Таблица 1: Видове обществени поръчки (таксономия на активите)

Вид обществена поръчка	Описание на вида
Клинични информационни системи	Включва обществени поръчки за всякакъв вид софтуер, предназначен за медицински грижи
Медицински изделия	Всякакъв хардуер, предназначен за лечение, контрол или диагностициране на заболявания
Мрежово оборудване	Мрежови линии (коаксиални, оптични), портали, маршрутизатори, превключватели, защитни стени, VPN, IPS, IDS и др.
Системи за грижи от разстояние	Съоръжения или устройства за предоставяне на грижи извън болничната среда, особено такива, които днес се наричат „домашни грижи, базирани на болнични услуги“.
Мобилни клиентски устройства	Всеки софтуер, осигуряващ здравна помощ или събиране на медицински данни, който не е свързан директно с болничната мрежа; напр. приложения за телемедицина
Системи за идентификация	Системи за уникална идентификация на пациенти или медицински персонал (биометрични скенери, четящи устройства за карти и др.) и гарантиране на идентификация и/или разрешение за достъп до информационните системи.
Системи за управление на сгради	Всякакви видове конструкции, в които могат да се намират медицински съоръжения.
Системи за управление на индустриални процеси	Системи, които контролират всички физически аспекти на центрове, например системи за регулиране на електрозахранването, системи за заключване на вратите, вътрешни системи за сигурност.
Професионални услуги	Всички видове услуги, възложени или не на външни изпълнители и предоставяни от специалисти или дружества: медицински услуги, транспорт, счетоводство, инженеринг, информационни технологии, правни услуги, поддръжка, почистване, кетъринг и др.
Облачни услуги	Всяка КИС или друга информационна система, която не е разположена в медицинската сграда или в център за електронно обработване на данни и не е под пълния контрол на ИТ звеното на медицинския център.

ТАКСОНОМИЯ НА ЗАПЛАХИТЕ

Различните видове обществени поръчки са свързани с различни заплахи за ИКТ средата на болницата. Разгледайте таксономията на заплахите, представена в настоящия раздел, заедно с отдела по сигурност или риск на информационните технологии, за да определите кои заплахи са от най-голямо значение за вашата организация. Тази дейност следва да бъде част от ИТ задачите в болницата, независимо от вероятността за възлагане на обществени поръчки.

Таблица 2: Видове заплахи (таксономия на заплахите)

Заплаха	Примери
Природни явления	Пожар, наводнения или земетресения
Срив във веригата на доставки	Повреда при доставчик на облачни услуги, повреда при доставчик на мрежови услуги, повреда в електрозахранването, повреда при производител на медицински изделия/отказ от отговорност
Човешки грешки	Грешка в конфигурацията на медицинската система, липса на одитни записи, неразрешен достъп — контрол/липса или процеси, неспазване (BYOD), медицинска грешка/грешка на пациента
Злонамерени действия	Зловреден софтуер (вирус, софтуер за изнудване, BYOD), отвличане (крипто-отвличане, медицинско отвличане, социално инженерство (фишинг, бейтинг, клониране на устройства), кражба (данни, изделие), подправяне на медицински изделия, скиминг, отказ на услуга, уеб базирани атаки, атаки в уеб приложения, вътрешна заплаха, физическа манипулация/увреждане, кражба на самоличност, кибершпионаж, механично нарушаване на функциите на компонент
Неизправности на системата	Отказ на софтуера, остарял софтуер на производителя, повреда на устройството, повреда на мрежови компоненти, недостатъчна поддръжка

ДОБРИ ПРАКТИКИ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА ПРИ ВЪЗЛАГАНЕТО НА ОБЩЕСТВЕНИ ПОРЪЧКИ

Списъкът на добрите практики по-долу съвсем не е изчерпателен; но той дава солидно предимство на специалиста по информационни технологии в здравеопазването, който отговаря за закупуването на болнично оборудване. Наборът от добри практики е колективен резултат от всички мнения и предложения, получени от интервюираните медицински специалисти. Читателят може да адаптира списъка въз основа на приоритетите на своята организация.

ДП 1. Включване на ИТ отдела в различните етапи на възлагане на обществени поръчки, за да се гарантира, че се взема предвид експертният опит в областта на киберсигурността.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Всички

Свързани заплахи: Всички

ДП 2. Прилагане на процедура за идентифициране и управление на уязвимостта, за да се гарантира, че уязвимостта се взема предвид преди снабдяването с нови продукти или услуги и че уязвимостта на съществуващите продукти/услуги се наблюдава през целия им жизнен цикъл.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Клинични информационни системи, медицински изделия, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Всички

ДП 3. Разработване на политика за актуализиране на хардуера и софтуера, за да се гарантира, че се прилагат най-новите корекции на вашата ОС и софтуер и антивирусният софтуер се актуализира.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 4. Засилване на контрола за сигурността на безжичните комуникации, за да се гарантира, че достъпът до безжичните мрежи на болницата е ограничен и строго контролиран.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Медицински изделия, мобилни клиентски устройства, системи за идентификация, облачни услуги

Свързани заплахи: Злонамерени действия, човешки грешки

ДП 5. Установяване на политики за тестване, за да се гарантира, че новопридобити или новоконфигурирани продукти се подлагат на изпитания за пробив, а предприетите коригиращи действия са в съответствие с оперативните параметри на реалната среда.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Клинични информационни системи, медицински изделия, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на сгради, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, неизправности на системата, човешки грешки

ДП 6. Изготвяне на планове за непрекъснатост на дейността, за да се гарантира, че неизправности в дадена система няма да нарушат основните услуги на болницата и че ролята на доставчика е ясно определена.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 7. Да се вземат предвид въпросите, свързани с оперативната съвместимост, за да се гарантира, че няма пропуски по отношение на сигурността на вече съществуващите компоненти (наследени ИТ).

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Клинични информационни системи, медицински изделия, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Неизправности на системата, човешки грешки, злонамерени действия

ДП 8. Да се даде възможност за тестване на всички компоненти, за да се гарантира, че изпълняват обещаните функции: проверка за лесна употреба, проверка на точността на резултатите при натоварване и проверка за пропуски в сигурността (политика на слаби пароли, въвеждане на SQL)

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Клинични информационни системи, медицински изделия, устройства за клиенти от разстояние, системи за идентификация, облачни услуги, системи за управление на индустриални процеси, система за грижи от разстояние, системи за управление на сгради, мобилни клиентски устройства

Свързани заплахи: Злонамерени действия, човешки грешки, неизправности на системата, срив във веригата на доставки

ДП 9. Да има възможност за извършване на одит и регистриране, за да се проследяват извършителите на атаки и да се следи какво количество информация е изгубена/откраднатa, когато системата е била компрометирана.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Медицински изделия, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 10. Криптиране на чувствителни лични данни в покой и при пренос, като бъде определена политика за системите, услугите или устройствата, обработващи специалните категории лични данни съгласно член 9 от ОРЗД.

Етапи на възлагане на обществени поръчки: Всички

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 11 Извършване на оценка на риска като част от процедурата за възлагане на обществена поръчка.

Етапи на възлагане на обществени поръчки: Планиране

Свързани видове обществени поръчки: Всички

Свързани заплахи: Всички

ДП 12. Предварително планиране на мрежовите, хардуерните и лицензионните изисквания, за да се определи дали трябва да бъдат направени допълнителни обновявания и/или покупки преди инсталирането с цел приспособяване на новата система.

Етапи на възлагане на обществени поръчки: Планиране

Свързани видове обществени поръчки: Клинични информационни системи, мрежово оборудване, системи за идентификация, системи за управление на индустриални процеси

Свързани заплахи: Срив във веригата на доставки, неизправности на системата, природни явления, човешки грешки

ДП 13. Идентифициране на заплахите, свързани с обществените поръчки за продукти или услуги и гарантиране, че това се извършва непрекъснато през целия жизнен цикъл на обществените поръчки.

Етапи на възлагане на обществени поръчки: Планиране, управление

Свързани видове обществени поръчки: Всички

Свързани заплахи: Всички

ДП 14. Разделяне на мрежата, за да се гарантира, че мрежовият трафик може да бъде изолиран и/или филтриран с цел ограничаване и/или предотвратяване на достъпа между зоните на мрежата.

Етапи на възлагане на обществени поръчки: Планиране, възлагане

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 15. Определяне на мрежовите изисквания, за да се гарантира оперативната съвместимост и да се избегнат пропуски след създаването на топологията на мрежата и компонентите.

Етапи на възлагане на обществени поръчки: Планиране

Свързани видове обществени поръчки: Клинични информационни системи, мрежово оборудване, системи за идентификация, системи за управление на индустриални процеси, облачни услуги, системи за грижи от разстояние, мобилни клиентски устройства

Свързани заплахи: Срив във веригата на доставки, неизправности на системата, природни явления

ДП 16. Определяне на основни изисквания по отношение на сигурността и превръщането им в критерии за допустимост при избора на доставчици.

Етапи на възлагане на обществени поръчки: Планиране, възлагане

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 17. Създаване на специална покана за оферти за възлагане на поръчки за облачни услуги, като се вземат предвид регулаторните изисквания и изискванията на политиките.

Етапи на възлагане на обществени поръчки: Планиране, възлагане

Свързани видове обществени поръчки: Облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки

ДП 18. Приоритизиране на възлагането на обществени поръчки за активи, които са сертифицирани по схеми/стандарти за киберсигурност.

Етапи на възлагане на обществени поръчки: Възлагане

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 19. Извършване на оценки на въздействието върху защитата на данните при планиране на възлагане на поръчки за нова система или услуга.

Етапи на възлагане на обществени поръчки: Възлагане

Свързани видове обществени поръчки: Клинични информационни системи, медицински изделия, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, професионални услуги, облачни услуги

Свързани заплахи: Злонамерени действия, човешки грешки

ДП 20. Създаване на портали, които поддържат връзката със заварени системи/машини и осигуряват граничен контрол в случай на проблеми вътре в тези групи.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Медицински изделия, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 21. Предоставяне на обучение в областта на киберсигурността относно практиките на организацията в тази област, за да се гарантира, че вътрешният персонал или външните изпълнители/консултанти, работещи на място, са подходящо обучени.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Всички

Свързани заплахи: Злонамерени действия, човешки грешки

ДП 22. Разработване на планове за реагиране при инциденти, които обхващат новопридобити продукти или системи.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 23. Включване на продавача/производителя в управлението на инциденти и определяне на ясни условия в поканата за оферти.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 24. Планиране и наблюдение на дейностите по поддръжка на цялото оборудване, за да се гарантира адекватно ниво на функционалност и вземането на решения за евентуални обновявания/корекции и т.н.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Клинични информационни системи, мрежово оборудване, медицински изделия, системи за управление на сгради, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Човешки грешки, неизправност на системата, природни явления

ДП 25. Отдаленият достъп следва да бъде сведен до минимум и администриран по такъв начин, че външната комуникация с доставчика да бъде ограничена само до устройството, което той трябва да управлява.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата, човешки грешки

ДП 26. Изискване на корекции за всички компоненти и включване на информация за това в поканата за оферти.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата

ДП 27. Повишаване на осведомеността на персонала относно киберсигурността, за да се гарантира, че той е запознат с рисковете, свързани с новопридобити продукти или услуги.

Етапи на възлагане на обществени поръчки: Управление

Свързани видове обществени поръчки: Всички

Свързани заплахи: Всички

ДП 28. Управление на наличностите на активите и конфигурацията, за да се гарантира, че запасите се обновяват по подходящ начин, когато даден компонент се добавя или изважда от ИКТ средата, и че са налице основните конфигурации за сигурност за ИКТ компонентите и те се управляват по подходящ начин.

Етапи на възлагане на обществени поръчки: Управление

Свързани видове обществени поръчки: Клинични информационни системи, медицински изделия, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация

Свързани заплахи: Злонамерени действия, човешки грешки, неизправности на системата

ДП 29. Създаване на специални механизми за контрол на достъпа до съоръжения за медицински изделия, които следва да бъдат също физически защитени и достъпни само за специализиран персонал.

Етапи на възлагане на обществени поръчки: Управление

Свързани видове обществени поръчки: Медицински изделия, системи за управление на сгради, системи за идентификация

Свързани заплахи: Злонамерени действия, човешки грешки

ДП 30. Планиране на чести изпитвания за пробиви по график или след промяна в архитектурата/системата и включване на условията и сроковете в поканата за оферти.

Етапи на възлагане на обществени поръчки: Възлагане, управление

Свързани видове обществени поръчки: Медицински изделия, клинични информационни системи, мрежово оборудване, система за грижи от разстояние, мобилни клиентски устройства, системи за идентификация, системи за управление на индустриални процеси, облачни услуги

Свързани заплахи: Злонамерени действия, срив във веригата на доставки, неизправности на системата