МАТРИЦА ЗА ОДИТ НА КИБЕР РИСКА

ENCRYPT 4.0

Съфинансирано от Европейския съюз

Проектът ENCRYPT4.0 (2020-1-RO01-KA202-079983) е финансиран с подкрепата на Европейската комисия. Настоящата публикация отразява само вижданията на автора, а Комисията не носи отговорност за използването на съдържащата се в нея информация.

Съдържание

1. ВЪВЕДЕНИЕ

Увеличената свързаност благодарение на Индустрия 4.0, използването на цифрови изчисления и съхранение на данни извън обектите се развива потенциал за генериране на конкурентни предимства по отношение на производителността, качеството и разходите за производство. Налице са обаче и свързаните рискове за производствени МСП, като потенциални конкуренти и достъп до данни. Кибер атаките стават все повече и по-чести и обикновено се правят с цел извличане или кражба на поверителни или фирмени данни, манипулиране на събраните данни за причиняване на нежелани ефекти и унищожаване на капиталови активи (Margot Hutchins & Stefanie Robinson, 2015). Кибер атаките могат да се дефинират като „атака, в кибер пространството, която е насочена към използването на това пространство от дадено предприятие с цел нарушаване, обездвижване, унищожаване или злонамерен контрол на компютърна среда/инфраструктура, или унищожаване целостта на данните или кражба на контролирана информация“ (National Institute for Standards and Technology, 2012, p. B3). Световният икономически форум (2017) приоритизира две решения за адресиране на свързани с иновациите кибер рискове: i) измерване на кибер риска и ii) оценка на кибер сигурността. През 2019 г. измамите и кражбите на данни и кибер атаките са идентифицирани от Форума като четвърти и пети най-вероятни рискове (World Economic Forum, 2020), а през 2020 рисковете, свързани с кибер пространството, като кибер атаки и измама или кражба на данни, са в топ 10 на дългосрочните рискове.

Проектът ENCRYPT 4.0 се фокусира върху оценка на кибер сигурността чрез разработване на матрица за оценка на кибер рискове.

Производствената промишленост се нуждае от инструменти за включване на кибер рисковете в съществуващите си процеси на управление на риска. В този контекст, ENCRYPT 4.0 адресира тази нужда, като се фокусира върху оценка на кибер сигурността чрез разработване на матрица за оценка на кибер рискове (Cyber Risk Audit Matrix). CRAM е подробен инструмент, който има за цел да подпомогне мениджърите в производствени МСП за извършване на пълен анализ на процесите с оглед използването на иновативни технологични решения, базирани на Индустрия 4.0, идентифициране на кибер рисковете и създаване и прилагане на ефективни контроли. CRAM разработена на базата на експертни познания относно национални, европейски и световни стандарти (Анекс А), както и обратна връзка от експерти в областта на кибер сигурност в шест европейски държави – Австрия, Португалия, Румъния, България, Кипър и Испания.

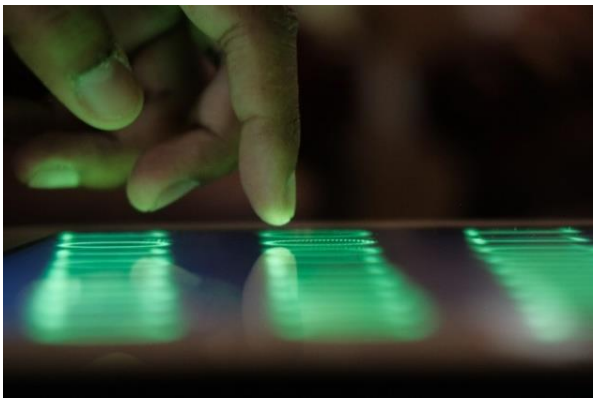
- Този документ съдържа: a) стойностно предложение на Матрицата, b) методология на Матрицата (CRAM), c) описание на категориите в матрицата за оценка на кибер рисковете, d) стъпки за провеждане на одит на кибер сигурността и e) библиография.

2. СТОЙНОСТНО ПРЕДЛОЖЕНИЕ НА МАТРИЦАТА

Матрицата за одит на кибер риска (CRAM) ще позволи на интелигентните фабрики да извършват системен преглед на своите кибер рискове и да създадат точен профил на риска от кибер заплахи. Матрицата по проект Encrypt 4.0 ще позволи на интелигентните фабрики да извършват последователни анализи на данни в реално време и да оценяват своите кибер рискове на базата на конкретна и всеобхватна матрица.

Матрицата е аналитичен инструмент, целящ да подпомага производствените компании в идентифицирането, анализа и приоритизирането на рискове, както и своевременното определяне на защитни мерки. През последните години един от най-належащите проблеми на дигиталния свят е кибер сигурността и защитата на поверителността на данните. През 2019 г. World Economic Forum (WEF) класира кибер атаките сред топ 5 на глобалните рискове.

През 2020 г., с оглед на пандемията от COVID-19, увеличената зависимост от свързаност и дигитална инфраструктура поради затварянето на икономически дейности увеличиха възможностите за кибер атаки и проникванията. Същевременно, за да се увеличат вредите и финансовите облаги, кибер престъпниците променят целите си и вместо към физически лица и малки бизнеси се насочват към големи корпорации, правителства и критична инфраструктура, играещи важна роля в реакцията на пандемията (INTERPOL G. S., 2020). „Кибер атаките са по-голяма опасност за демокрациите и икономиките от оръжията и танковете“ (Juncker, 2017).



Cybersecurity Ventures (2020), водещият изследовател в областта на глобалната кибер икономика, прогнозира, че „глобалните щети, свързани с кибер престъпност през 2021 г. ще достигнат 6 трилиона долара, което ще е повече от всички природни бедствия за година“. Официалният годишен доклад за кибер престъпност от 2019 г. посочва, че „в края на 2016 г. бизнесът е ставал жертва на атаки на всеки 40 секунди“ (Cybersecurity Ventures, 2019), а очакванията са честотата да се увеличи до 11 секунди през 2021 г.

Кибер атаките спрямо критична инфраструктура, класирани на пето място сред рисковете, определени от мрежа от експерти на WEF, се превръщат в новата нормалност в редица сектори, като енергетика, здравеопазване и транспорт. Производството обаче е обект на все повече кибер атаки, както показва доклада от разследвания на неправомерен достъп до данни за 2020 г., като посочва, че е имало 922 инцидента 381 от които с потвърдено разкриване на данни, само в САЩ (Verizon, 2020). Организираната кибер престъпност набира сила и вероятността от разкриване и разследване е едва 0.5% в САЩ, „кибер престъпността като услуга е развиващ се бизнес модел, като увеличаващото се усложняване на инструменти в Darknet прави услугите по-достъпни за всички“ (World Economic Forum, 2020).

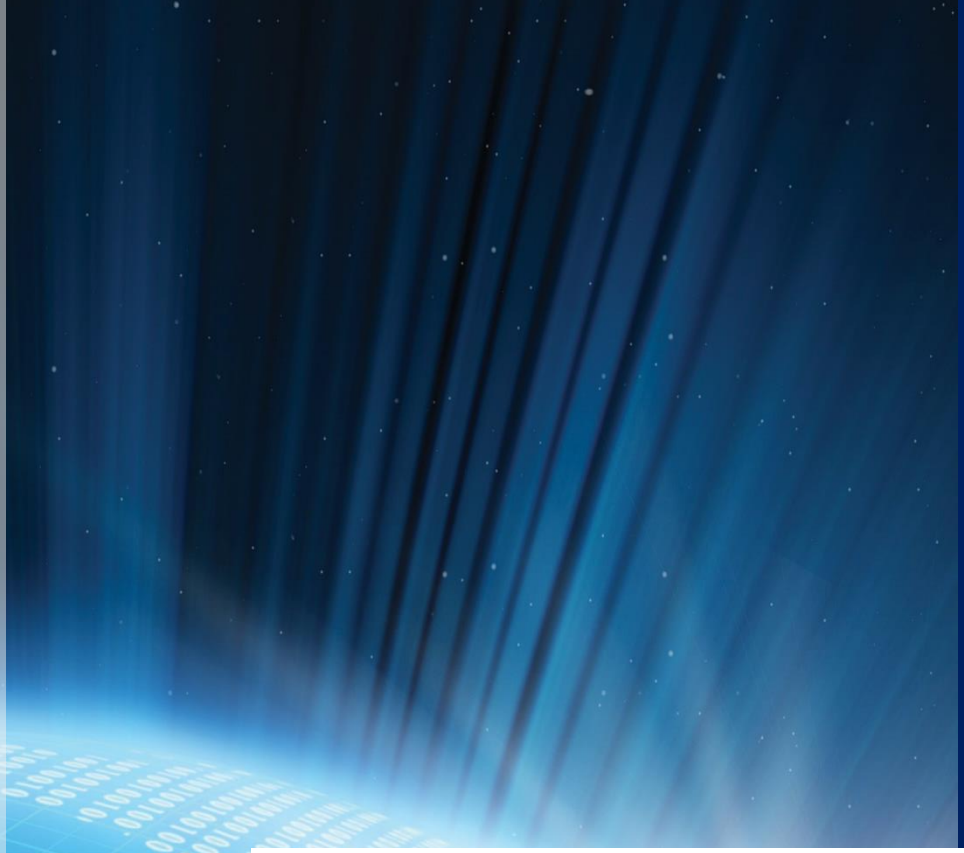
Възможностите за отбрана на МСП обикновено са по-малки от тези на големите предприятия; данните показват, че едва 14% от засегнатите МСП могат да се възстановят сами. National Cyber Security Alliance посочва, че 60% от МСП, които стават обект на кибер атака, губят бизнеса си в рамките на 6 месеца, както и че „производителите са по-изложени на заплахи за сигурността поради свързаността в ИТ и ОТ (оперативни технологии) чрез дигитализацията на Индустрия 4.0 (Verizon, 2017).

Повечето производствени компании в усилията си да запазят конкурентните си предимства, при адаптиране на практики, базирани на Индустрия 4.0, правят откъслечни инвестиции в системи за контрол и външни консултанти, но им липсва интегриран подход за управление на кибер рисковете. Усилията им не успяват ефективно да се справят с бързо развиващите се кибер заплахи, защото повечето производствени системи традиционно са фокусирани върху безопасността и резултатността, а не върху сигурността. Когато става дума за сигурност, производителите в миналото обикновено са загрижени за подсигуряване на ОТ средата и често пренебрегват ИТ сигурността, докато „появата на Индустрия 4.0 въвежда нови технологии в традиционните ОТ среди, така че хората, запознати с работата с ОТ в такива среди трябва да се адаптират“ (EU Agency for Cybersecurity, 2019). Служителите често използват противоречива информация, за да описват или оценяват някои аспекти на кибер риска.

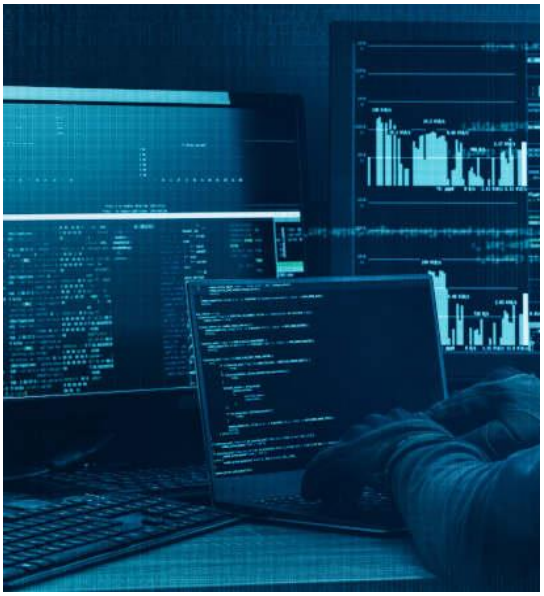
Матрицата съдържа ключови индикатори на риска, които са лесно приложими към данни в реално време. CRAM ще позволи на служителите не само да изготвят дългосрочна стратегия за оценка на кибер сигурността, но и за бързо извършване на ежедневната отчетност. Това ще показва реалните нива на риск за процесите във всеки момент, което е от особена важност за поддържането на текущото производство, тъй като най-малкото забавяне на даден процес може да има необратим ефект и да доведе до огромна финансова загуба. Рисковете за сигурността в производството стават все по-комплексни, повишавайки нуждата от адекватен аналитичен инструмент, с чиято помощ МСП да определят предпазни мерки, които да се прилагат ежедневно в производствена среда. За разлика от неизправностите в механичните процеси, които могат да се категоризират като статични, тези в кибер сигурността са динамични, тъй като са тясно свързани с човешко взаимодействие.

Основната цел на **CRAM е да осигури на ръководителите в производството информация относно потенциални рискове за кибер сигурността в техните системи и да им помогне да приложат ефективна стратегия за ограничаване на рисковете.** Предвид ограничените изследвания в областта на оценка на риска за кибер сигурността, разработената Encrypt 4.0 матрица представлява иновативен инструмент, който може да бъде включен в политиката за управление на риска на производствените компании

Матрицата за одит на кибер риска съдържа ключови индикатори на риска, които са лесно приложими към данни в реално време.



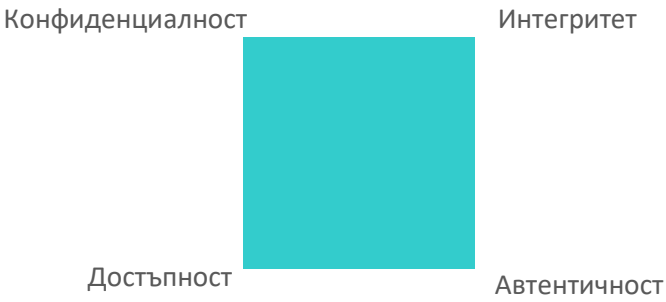
Основната цел на Матрицата (CRAM) е да предостави на ръководителите на производства инфорация относно потенциалните рискове за киберсигурността в системите им и да ги подпомогне в прилагането на ефективна стратегия за ограничаване на рисковете.



Матрицата (CRAM) се основава на квартета CIAA

3. МЕТОДОЛОГИЯ НА МАТРИЦАТА

Матрицата (CRAM) е разработена на базата на квартета на **CIAA** - **конфиденциалност, интегритет, достъпност и автентичност.** Тя измерва два основни аспекта: **Вероятност на риска и Влияние на риска,** адаптирани спрямо конкретните нужди на производствените МСП, като дава възможност лесно да се съобразят с организационната култура на компаниите



Матрицата (CRAM) също така включва: i) пореден номер на риска, ii) категория на риска, iii) източник на риска, iv) описание на риска, v) потенциални разходи, свързани с последствията от риска, vi) отдели в организацията, които може да бъдат засегнати, vii) смекчаване/вече извършени действия, viii) ефект от риска, ix) вероятност на риска, x) цялостно ниво на риска, xi) задействащи фактори, xii) предстоящо смекчаване/действия, xiii) потенциални разходи за смекчаване, xiv) краен срок, xv) отговорник за управлението на риска, xvi) супервайзер, отговорен за мониторинг, както и xvii) оценка на ефективността.

По-долу е дадено описание на основните понятия, които съставляват матрицата за оценка от кибер рисковете:

Достъпност: Гарантиране на навременен и надежден достъп до информация.

Автентичност: Гарантиране истинността и оригиналността на данните, възможност за верификация и надеждност на пренос, съобщение или подател (Проект Encrypt 4.0, 2020).

Оценка на кибер сигурността: Конкретни насоки за кибер сигурност и механизми за оценяване, включително общи принципи за оценка на кибер сигурността, механизъм за оценяване с точки и практически стъпки за подобрения, които позволяват на компаниите да оценят и подобрят своята кибер сигурност (World Economic Forum , 2017).

Поверителност: Запазване на (контролирани) ограничения на достъпа и разкриването на информация, включително мерки за защита на личната поверителност и информация за собствеността.

Влияние: Оценението потенциален ефект от компрометиране на поверителността, целостта или наличността на вид информация, изразени като стойности *ниско, средно или високо*.

Интегритет: Защита от неправилна промяна или унищожаване на информация, включва гарантиране целостта и истинността на информацията.

Вероятност: Тежестен фактор, базиран на субективен анализ на вероятността от дадена заплаха спрямо уязвимост или набор от уязвимости.

Описанията са вдъхновени от Наръчника за провеждане на оценки на риска (Национален институт за стандарти и технологии, 2021 г.).

4. МАТРИЦА ЗА ОЦЕНКА НА КИБЕР РИСКА (CRAM)

Матрицата (CRAM), разработена по проект Encrypt 4.0 представлява подробен инструмент, който има за цел да подпомогне мениджърите в производствени МСП за извършване на пълен анализ на процесите с оглед използването на иновативни технологични решения, базирани на Индустрия 4.0, идентифициране на кибер рисковете и създаване и прилагане на ефективни контроли.

4.1 КАТЕГОРИИ В МАТРИЦАТА ЗА ОДИТ НА КИБЕР РИСКА

Тези категории са базирани на проучване и анализ на над 20 стандарта (Анекс А) в областта на информационната сигурност и защитата на данните, както и на проведени 12 подробни интервюта с експерти в областта на кибер сигурността от Австрия, Португалия, Румъния, България, Кипър и Испания.

Таблица 1. Категории в Матрицата за одит на кибер риска

Категория риск	Описание на категорията
Човешки ресурси	Идентифициране на рисковете, свързани с човешките ресурси в компанията. Рисковете, които са свързани с ролите и отговорностите на персонала, вземане на решения, управление на самоличност, контрол на достъп, повишаване на информираността.
Интелектуална собственост	Идентифициране на рисковете, свързани с интелектуалната собственост на компанията. Интелектуалната собственост включва индустриална собственост, авторско право и свързани права и се отнася до правото на изключително ползване на съответната техническа, търговска и промишлена информация. Индустриалната собственост има за цел да защити изобретения, патенти, търговски марки и проекти за ексклузивно използване, права върху производството и маркетинга.
Сигурност на системи за индустриален контрол (ICS)	Сигурността на системите за индустриален контрол включва пазене и подсигуряване на системите, както и необходимия софтуер и хардуер, които се използват от тях.
Продукти	Идентифициране на рисковете, свързани с продуктите. Появата на този риск може да застраши произвежданите от организацията продукти.
Законови рискове за киберсигурността	Идентифициране на рисковете, свързани със законови и регулаторни отговорности. Появата на този риск може да застраши законовите и/или регулаторни отговорности на организацията.
Атаки спрямо веригите на доставки	Идентифициране на уязвими аспекти по веригата на доставки. Организацията трябва да дефинира, оцени и управлява процесите на оценка на риска по веригата на доставки и логистиката. Идентифициране на връзки с доставчици със слаба сигурност.
Технологии, ИКТ и оперативна безопасност	Идентифициране на рисковете, свързани с технологии, ИКТ и дейността на компанията. За да се управляват опасностите, произтичащи от функционален недостатък на операции, оперативни прекъсвания или чрез предвиждане на неправилно използване/грешки от сътрудници във връзка с технологии, ИКТ и операции.
Клиенти	Появата на даден риск може да застраши услугата, предоставена на клиентите, или да компрометира данните на клиентите.
Физическа киберсигурност	Физическата киберсигурност е защитата на кибер-физически системи, устройства свързани посредством Интернет на нещата, защита на хора, собственост и физически активи от действия и събития, които могат да причинят щети или загуба.

5. ОДИТИ НА КИБЕРСИГУРНОСТТА

5.1 КАКВО ПРЕДСТАВЛЯВА ОДИТЪТ НА КИБЕРСИГУРНОСТТА?

Четвъртата индустриална революция, или Индустрия 4.0, носи редица промени и нови технологии, които свързат физическия и дигиалния свят в рамките на бизнес процесите в интегрирани интелигентни системи. Това осигурява много възможности за подобряване на процесите и цялостното представяне, но и много нови отговорности и заплахи. По-високото ниво на свързаност между всички системи посредством интернет на нещата, облачни технологии и много други, наред с многото ползи носи и нови предизвикателства за компаниите, свързани със сигурността на информацията, големи данни и др., които се обработват от тези интегрирани системи. Именно затова компаниите и особено МСП се нуждаят от инструменти, които да им помогнат в процеса на проверка и анализ на техните слабости, когато става дума за сигурност на технологиите, базирани на Индустрия 4.0. Ефективен инструмент за такава проверка е провеждането на одит на кибер сигурността.

Одитът на киберсигурността представлява оценка на представянето спрямо спецификации, стандарти, контроли или насоки.

Одитът на киберсигурността представлява оценка на представянето спрямо спецификации, стандарти, контроли или насоки (CyLumena, 2020). Одитите на киберсигурността обикновено се извършват по чеклист от контроли (библиотека с контроли), дефинирани на базата на определени стандарти за киберсигурност (национални, международни, вътрешни за компанията) и/или процедури и/или политики на компанията. Целта на одита на киберсигурността е да помогне на организациите да оценят дали разполагат с подходящи механизми за сигурност, като идентифицират пропуски в сигурността или валидират прилаганите процедури и политики. Одитите на кибер сигурността помагат на бизнесите да проверят какво има в мрежата им, кое трябва да бъде защитено и какви пропуски има в съществуващата защита, за да могат да направят подобрения (Dosal, 2020).

ОДИТ НА КИБЕССИГУРНОСТТА VS. ОЦЕНКА НА КИБЕРСИГУРНОСТТА

Одитите на киберсигурността се различават от оценките на киберсигурността. Докато одитите проверяват дали са налице определени контроли, оценката има за цел да оцени ефективността на тези контроли (Aldorisio, 2020). Оценките може да включват известна степен на одит, но не винаги. Одитите на киберсигурността, в зависимост от целта им, могат да се прилагат, когато една организация иска да оцени своето съответствие с определени закони или други стандарти; в този случай обикновено одитът се провежда от трета външна страна, която има необходимата компетенция. Оценките на кибер сигурността, от друга страна, могат да се провеждат вътрешно от хора в организацията, които имат добри познания за инфраструктурата за киберсигурност.

ВЪНШНИ И ВЪТРЕШНИ ОДИТИ НА КИБЕРСИГУРНОСТТА

Външните одити се извършват от професионалисти, особено с цел основания за сертификация по определени стандарти и оценка на съотвтетсвието спрямо официални стандарти, закони и др. Вътрешните одити на киберсигурността (одити от първа страна) могат да се провеждат от вътрешен експерт, който е добре запознат с процесите на компанията и архитектурата на киберсигурността. Според GDPR (GDPR.EU N.d.), всяка компания има законово задължение да има номиниран Отговорник за защита на данните, който

е наясно с управлението на данните – каква информация постъпва в и излиза от компанията, в какви процеси се използва и как се използва. Следователно, естествен избор за провеждането на вътрешен одит на киберсигурността може да е избрания отговорник за защита на данните или специализирана компания, в зависимост от обхвата на одита. В следващите раздели на настоящия документ ще представим комбиниран подход към провеждане на вътрешен одит на киберсигурността и оценка на базата на споменатите по-рано категории, които трябва да се вземат предвид в процеса на одит.

5.2 КАК СЕ ПРОВЕЖДА ВЪТРЕШЕН ОДИТ НА КИБЕРСИГУРНОСТТА?

Целта на този раздел е да предостави лесни насоки за провеждане на вътрешен одит на киберсигурността, който може да изпълнява ролята на ефективен инструмент за оценяване на сигурността на данните и киберсигурността в организацията и/или като подготовка за външен одит на киберсигурността.

СТЪПКА 1: Дефинирайте приоритетите за сигурност на своята организация и обхвата на одита

На този етап лицето или екипът, които ще проведат одита, трябва да идентифицират обхвата на процеса на одит. Добра отправна точка е да се изброят всички кибер активи на компанията, като кибер активи, свързани с критична инфраструктура като: системи за контрол, системи за придобиване на данни; мрежово оборудване, хардуерни платформи за виртуални машини или съхранение; вторични или поддържащи системи като скенери за вируси, отопление, вентилация и климатизация (ОВК) и непрекъснато захранване (UPS) (n.d., Versify Solutions);

След това трябва да оцените кои са критичните кибер активи (Critical Cyber Assets - CCA). Според стандарта за защита на критичната инфраструктура (CIP), версия 4 на North American Electric Reliability Corporation (NERC), критичен кибер актив (CCA) е „всяко устройство, което използва проследим протокол за комуникация извън периметъра на електронна сигурност (ESP), използва проследим протокол в контролен център или има комутируем достъп.”(2011, Flick & Morehouse).

По-просто казано, активите могат да варират от компютърно оборудване до различни системи и чувствителна информация за клиентите и компанията, вътрешна документация и комуникационни системи.

След като бъдат идентифицирани критичните кибер активи, трябва да идентифицирате критичните параметри на сигурността и да сегментирате какво ще бъде включено в обхвата на одита (2019, LeCount). Параметрите и активите зависят от компанията, следователно тази начална стъпка и правилната дефиниция на обхвата на одита са много важни за ефективността на процеса на одит. След като обхватът на одита бъде дефиниран, може да продължите към следващата стъпка – идентификация на потенциалните заплахи.

СТЪПКА 2: Идентифициране на потенциалните рискове и заплахи

На базата на дълбочинни интервюта с 12 експерти в областта на киберсигурността, консорциумът по проект ENCRYPT 4.0 е идентифицира девет възможни рискови категории и състави списък с възможни заплахи, които всяка от тези категории може да носи за критичните кибер активи. Моделът ENCRYPT 4.0 включва следните 9 категории: (1) Човешки ресурси; (2) Интелектуална собственост; (3) Сигурност на системи за индустриален контрол (ICS); (4) Продукти; (5) Законови рискове за киберсигурността; (6) Рискове по веригата на доставки; (7) Технологии, ИКТ и оперативна безопасност; (8) Клиенти; (9) Физическа киберсигурност. Имайте предвид, че в зависимост от бизнес дейностите на организацията, бизнес модела и сектора, не

всички категории може да са приложими за вас или може да решите, че нямате критични кибер активи, свързани с тези категории. За да оцените това, прегледайте Анекс 1 и изберете съответните категории във вашата организацията, както и свързаните заплахи в зависимост от идентифицираните критични кибер активи.

СТЪПКА 3: Приоритизиране на рисковете

В тази важна стъпка трябва да проверите списъка с потенциални заплахи, които според вас са приложими за вашата компания, и според набор от критерии да прецените кои рискове са силно вероятни и е възможно да имат по-сериозен негативен ефект. Поради тази причина консорциумът по проект ENCRYPT 4.0 е разработил методология за оценка на риска, която разглежда следните компоненти:

- Потенциални разходи, свързани с последствията от риска;
- Отдел(и) в организацията, които може да бъдат засегнати;
- Потенциален ефект;
- Вероятност – при оценка на вероятността се разглеждат тенденции в сектора и предишни нарушения на сигурността;
- Ниво на риск.

Може да използвате директно матрицата за оценка на риска за киберсигурността ENCRYPT 4.0 (CRAM), разработена за лесно приоритизиране на потенциални рискове.

СТЪПКА 4: Одит на настоящите мерки за сигурност

След като сте идентифицирали приложимите категории рискове и заплахите за своята организация, следващата стъпка е да оцените дали вашите критични кибер активи и инфраструктура са уязвими на някоя от тези заплахи. За тази цел, трябва да оцените наличните протоколи/процедури/мерки за сигурност с цел идентифициране на потенциални пропуски в сигурността, които трябва да бъдат адресирани. В таблица 2 ще намерите насочващи въпроси и съвети за това как да оцените дали прилаганите мерки за сигурност са адекватни, но зависи и от заплахите, които според вас са приложими във всяка категория

Таблица 1. Съвети за идентифициране на текущи мерки за сигурност

№	Категория	Съвети за одит на текущите мерки за сигурност
1	**Човешки ресурси**	Проверете разпределението на роли и отговорности във връзка с управлението на данните и сигурността; киберсигурността; контрола на системи и др. Говорете с определените отговорници в тези области – попитайте ги как биха реагирали в определени ситуации, какви протоколи за сигурност биха изпълнявали, за да може да оцените дали персоналът е запознат и подготвен при евентуална реализация на определени рискове за киберсигурността; дали се нуждае от обучение или не. Анализирайте инциденти и случаи на нарушаване на сигурността поради грешки на служителите и начина, по който са били разрешени. Помислете дали има още нещо, което може да се направи, за да се минимизира появата на тази заплаха в бъдеще.
2	**Интелектуална собственост**	Проверете разпределението на ролите и отговорностите във връзка с управлението на интелектуална собственост, като търговски тайни и др. Интервюирайте отговорните служители, прегледайте съответната документация относно защитата на активи чрез патенти, търговски марки или други права на интелектуална и индустриална собственост. Как се поддържа и управлява тази документация, кой има достъп до нея? Имало ли е инциденти в миналото, свързани с изтичане на информация, липсваща информация в тази област? Как са били управлявани, обновен ли е протоколът за сигурност?
3	**Сигурност на системи за индустриален контрол (ICS)**	Кой има отдалечен и/или физически достъп до системите за индустриален контрол? Как се администрира отдалечения достъп до системите за индустриален контрол? Има ли контроли на сигурността като проверка на самоличността, контрол на достъпа и криптиране с цел защита от неупълномощен достъп до и използване на тези системи? Какви са мерките за контрол на физическия достъп? Има ли защитни стени за системите за индустриален контрол, протокол за повишаване контрола на достъп до трафика в мрежата на тези системи? Имате ли налична система за предотвратяване на неправомерен достъп?

4	**Продукти**	В зависимост от производствения процес на продуктите, трябва да определите в кои процеси се използва чувствителна информация и как се управлява и администрира тя. Има ли търговски тайни, свързани с производството на продукти и др.? Как компанията гарантира, че тази информация се управлява безопасно? Какъв е протоколът – роли и отговорности, процедури и др.? Има ли контрол на физически и дистанционен достъп до компютри и мрежи; производствени системи и др.? Как се осигурява и контролира?
5	**Законови рискове за киберсигурността**	Има ли контрол на физически и отдалечен достъп до компютри и мрежи на компанията? Как се осигурява и контролира? Как се управляват и администрират законовите данни? Сървърът подсигурен ли е? Кой има достъп до тази информация? Имало ли е пробив на сигурността в миналото? Как е бил управляван? Има ли начин за подобряване на протоколите за сигурност на базата на последни тенденции/събития/технологични развития?
6	**Атаки по веригата на доставки**	Кой има достъп до системите за управление на доставките? Има ли управление чрез привилегирован достъп? Кой има достъп до чувствителни данни? Как се подсигурява този достъп? Използват ли се Honeytokens? Какво е нивото на контрол върху достъпа на доставчици на услуги? Колко доставчици имат достъп до софтуера ви? Мрежата на доставчиците следи ли се за уязвими аспекти?
7	**Технологии, ИКТ и оперативна безопасност**	Има ли строги политики по отношение на мобилна сигурност и предпазване на данните? Актуализирани ли са всички софтуерни приложения и операционни системи? Прилага ли се контрол на достъпа по отношение на критичните активи за киберсигурността? Следи ли се активността на потребителските профили, вход и достъп до мрежата? Правилно ли са конфигурирани защитните стени, има ли end-to-end криптиране за чувствителни данни?

		Има ли механизми за разпознаване и избягване на атаки като phishing и pharming?
8	**Клиенти**	Кой има достъп до важните данни на клиенти? Имате ли резервни копия на важни бизнес данни и информация?
9	**Физическа киберсигурност**	Как се управлява поддържането на оборудването и критичните активи за киберсигурността? Кой има физически достъп до оборудването и критичните активи на кибер сигурността? Как се подсигурява този достъп?

СТЪПКА 5: Определяне/обновяване на протоколи за сигурност на базата на одита

При изпълнение на СТЪПКА 4 трябва да изготвите списък на идентифицираните заплахи, приложими за вашата организация, да знаете какво вече се прави и какво липсва, както и да идентифицирате адекватни протоколи за сигурност на информацията с цел неутрализиране или премахване на риска от заплаха (2020, LeCount).

Контролите на сигурността на информацията са мерки, които се предприемат с цел намаляване на рисковете свързани със сигурността на информацията, като изтичане на информация от системите, кражба на данни, както и неправомерни промени в дигитална информация или системи (Garcia, 2019). Основната цел на контролите на сигурността е да се защити достъпа, поверителността, автентичността и интегритета на данните и мрежите в компанията. Както беше отбелязано, контролите на сигурността обикновено се прилагат след оценка на риска и представляват желания резултат от оценките и одита на киберсигурността по отношение на адресиране на идентифицираните реални или потенциални пропуски в сигурността.

В таблица 3, наред с модела за оценка на риска за киберсигурността, разработен по проект ENCRYPT 4.0, на базата на интервюта с експерти в областта на киберсигурността от 6 европейски държави, сме идентифицирали два вида контроли – превантивни и коригиращи, за всяка от 9-те категории риск. На базата на одита, проведен в стъпка 4, вече сте запознати с наличните процедури за киберсигурност във вашата организация. В таблица 3 може да намерите предложения за превантивни и коригиращи контроли за всяка от категориите, които може да не се прилагат в организацията ви.

Таблица 2. Превантивни и коригиращи контроли за киберсигурност

Категория риск	Превантивни мерки (контроли)	Коригиращи мерки (контроли)
Човешки ресурси	Създаване на програма за обучения и информираност Ясно определяне от страна на ръководството на процедури за проверка на самоличност, проверка и контрол на достъпа	Контрол на разрешенията за потребители Прилагане на система за откриване на нарушения (IDS) за засичане на неупълномощен достъп до компютър или мрежа

Категория риск	Превантивни мерки (контроли)	Коригиращи мерки (контроли)
	Компанията трябва да има политика, която включва: ● Списък с позволен софтуер. ● Упълномощен набор от софтуери и регистър на лицензиите. ● Дисциплинарни санкции, свързани с неспазването на тези изисквания. Промяна на паролата на всяко тримесечие („политика за силна парола“) Разработване на решения за възстановяване при бедствия и планове за непрекъснатост на дейността	Смяна на всички пароли след възможно изтичане на данни Заключване на профили, за които се подозира неупълномощен достъп Настройка на двуетапна верификация, когато е възможно
Интелектуална собственост	Политики и отговорности за управление на интелектуалната собственост Всички приложими активи трябва да бъдат защитени с регистрирани патенти, авторски права и търговски марки. Съответните активи трябва да бъдат следени и защитени със застраховка. Разработени мерки, политики и отговорности за управление на репутацията.	Редовна оценка и обновяване на политики и отговорности Ако за регистриран патент липсва патент под условие, трябва да се получат търговска марка и авторски права Редовна оценка и обновяване на политики и отговорности
Сигурност на системи за индустриален контрол (ICS)	Разработване на мерки, политики, отговорности и бърза реакция в случай на инциденти	Редовна оценка и актуализиране на политиките и отговорностите
Продукти	Оценка на работните процеси Стандартизация и еволюция Контрол на физическия достъп до компютри и мрежови компоненти	Прилагане на многопластов подход за всеки риск или поне за рисковете, които имат висок потенциал в конкретния случай, за да има поне няколко слоя на защита, независимо дали става дума за технологии, служители, процеси, клиенти и др.

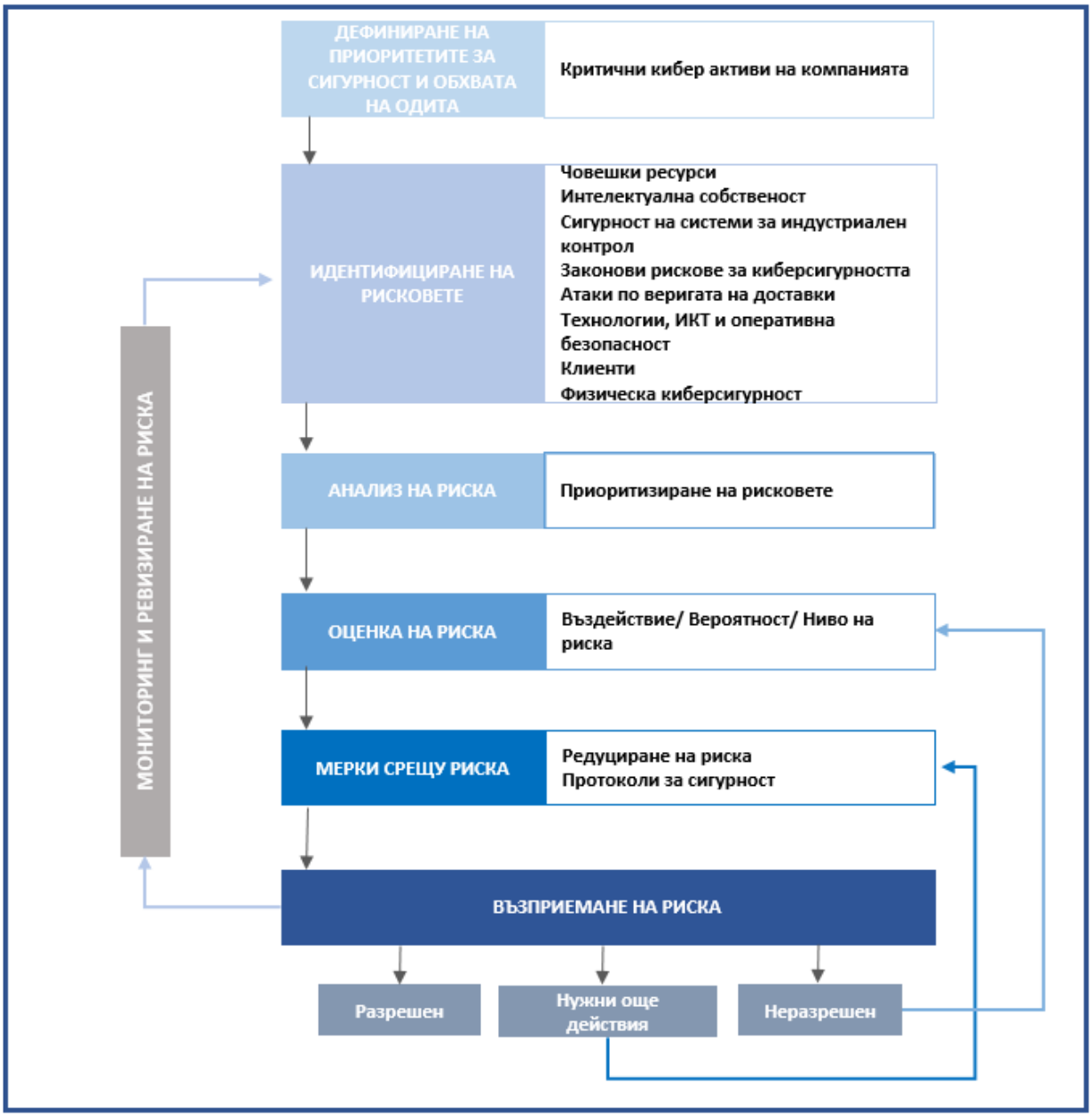
Категория риск	Превантивни мерки (контроли)	Коригиращи мерки (контроли)
Законови рискове за киберсигурността	Пазене само на необходимото. Инвентаризация на вида и количеството информация в наличните документи и компютри Предпазване на данните Унищожаване преди изхвърляне Обновяване на процедурите Образоване/обучение на служители Контрол на използването на компютри Подсигуряване на всички компютри	Идентифициране на засегнатите страни Уведомяване на засегнатите лица Правна консултация
Атаки по веригата на доставки	Използване Honeytokens Осигуряване на управление на привилегирован достъп Идентифициране на всички потенциални вътрешни заплахи Идентифициране и защита на уязвими ресурси Минимизиране на достъпа до чувствителни данни Изпращане на редовна оценка на риска на трети страни Мониторинг на мрежата на доставчици за уязвими аспекти Установяване на всяко изтичане на данни от доставчици	Проверка на лицензите по всички вериги на доставки на МСП Търсене на данни за контакт за превантивна и коректива поддръжка на машините в МСП за всички вериги на доставки и на регионално/местно ниво
Технологии, ИКТ и оперативна безопасност	Сваляне и инсталиране на актуализации на софтуера за операционните системи и приложения Обновяване на операционни системи и firmware Инсталиране на защитна стена (firewall) между интернет и LAN мрежата Идентифициране на критични активи	Проверка на всички оперативни системи и firmware в МСП и надзор на актуализациите Инсталиране на защитна стена (firewall) между интернет и LAN мрежата. Премахване на софтуер, който е незаконен или неразрешен според протокола на компанията

Категория риск	Превантивни мерки (контроли)	Коригиращи мерки (контроли)
	Информираност за сигурността Създаване на резервни копия и възстановяване Управление на уязвимостта Прилагане на контроли на достъпа Използване на филтри за съдържание и бял списък Правилно конфигуриране на крайни точки, установяване на процеси за реакция при инциденти Използване решения и системи за проверка на заплахи Правилно конфигурирани защитни стени, строги политики за мобилна сигурност, проверка на устройства за достъп до мрежата – това са някои практики за намаляване заплахата от използване на мобилни устройства в корпоративната мрежа. Достъп до софтуер с оглед на принципи за киберсигурност Гарантиране, че всички оперативни системи и всички софтуерни приложения са актуализирани Гарантиране, че чувствителните данни са криптирани Използване на софтуер за защита на данните Редовно следене активността на потребителските профили Управление на настройките за поверителност на мобилни приложения Прилагане на строги контроли върху устройствата за преносими данни	Стандартни инсталации за цялото компютърно оборудване Конфигуриране на VPN ако е необходимо отдалечено свързване Идентификация и коригиране на проблема. Одит и обновяване на политиките и правилата за сигурност.

Категория риск	Превантивни мерки (контроли)	Коригиращи мерки (контроли)
	Установяване на механизми за разпознаване и избягване на атаки като phishing и pharming. Дейност, базирана на политики и правила за сигурност.	
Клиенти	Създаване на резервни копия на важни бизнес данни и информация	Настройка на двуетапна верификация, когато е възможно Заключване на профили, за които се подозира неупълномощен достъп Блокиране на IP адресите на заподозрени източници на заплаха на базата на засечени дейности
Физическа кибер сигурност	Прилагане на план за безопасност в случай на пожар, наводнение, кражба, загуба… Изключване на инструменти или оборудване, които не се използват Резервно непрекъснато захранване или втори енергиен източник за аварийни ситуации Редовна проверка на всички устройства Създаване на резервни копия Хостване на всички данни в облака	Актуализация на безопасността на сградата и наличие на противопожарни мерки Резервно захранване за компютрите или втори енергиен източник Създаване на подсигурено копие Създаване на Safety switch Подмяна на повредени или аварирали устройства

ГРАФИЧНО ПРЕДСТАВЯНЕ НА ПРОЦЕСА С МАТРИЦАТА ЗА ОДИТ НА КИБЕР РИСКА (CRAM)

По-долу е дадено графично представяне на процеса на одит с помощта на Матрицата за одит на кибер риска (CRAM), разработена по проект Encrypt 4.0, като са показани съответните мерки, които следва да се предприемат от отговорника в производствените МСП за провеждане на подробен анализ на процесите чрез идентифициране на кибер рисковете и съдействие при проектирането и създаването на ефективни контроли съгласно прогресивното естество на кибер атаката.



Encrypt 4.0 CRAM е системен, продължителен процес. Това е цикличен процес, при който след идентифициране, анализ, оценка и адресиране на рисковете, следва мониторинг на риска и преглед. Ако проблемите продължават, трябва да се приложат допълнителни действия за разрешаването им, а затова е необходимо да се върнете към предходните стъпки в адресирането на риска.

6. ПРОЕКТ И ПАРТНЬОРИ

ENCRYPT 4.0

Съвместна инициатива за развитие на работна сила за подпомагане на европейската индустрия в преодоляването на недостига на професионалисти по киберсигурност

Проект ENCRYPT4.0 (2020-1-RO01-KA202-079983) има за цел да позволи на ръководствата на производствени МСП да възприемат проактивен подход към киберсигурността, като ги подкрепи в процеса на анализиране, идентифициране и справяне с кибер рисковете и заплахите, приложими за тяхната организация чрез промотиране на интерактивно базирано на проекти учене по отношение повишаване уменията за киберсигурност и компетенциите на служителите на МСП и/или професионалистите в сферата.

Университет по медицина, фармация, науки и технологии „Джеордж Емил Паладе“ - Търгу Муреш - Румъния

Координатор на проекта

Европейски център за качество ООД, консултантска компания - България

Instituto de Soldadura e Qualidade, технологичен институт - Португалия

Avantalia, технологично МСП - Испания

FH Joanneum, Университет за приложни науки - Австрия

PCX Management, Computers & Information Systems Ltd. - Кипър

ИЗТОЧНИЦИ НА ИНФОРМАЦИЯ

Aldorisio, J., 2020. Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]. Security Scorecard. Retrieved from https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit

Cybersecurity Ventures. (2019). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/annual-cybercrime-report-2019/

Cybersecurity Ventures. (2020). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

EU Agency for Cybersecurity. (2019). *Industry 4.0 Cybersecurity: Challenges & recommendations.*

European Union Agency for Cybersecurity. (2015). *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* ENISA. doi: 10.2824/829076

Juncker, C. P.-C. (2017). Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Margot Hutchins, R. B., & Stefanie Robinson, J. S. (2015). Framework for Identifying Cybersecurity Risks in. *U.S. Department of Energy*, 17.

National Institute for Standards and Technology. (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: Special Publication 800-30.

Verizon. (2017). *Verizon Data Breach Investigations Report.* Retrieved from https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

Verizon. (2020). *Manufacturing*. Retrieved from Verizon: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/

World Economic Forum . (2017). *Innovation-Driven Ciber-risk to Costumer Data in Financial Services.* Cologny/Geneva.

World Economic Forum. (2020). *The Global Risks Report.*

World Economic Forum. (2020). *Wild Wide Web - Consequences of Digital Fragmentation*. Retrieved from World Economic Forum: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

АНЕКС А - НАЛИЧНИ СТАНДАРТИ ЗА РИСКОВЕ СВЪРЗАНИ С КИБЕРСИГУРНОСТТА

Информационна сигурност (в различни индустрии)	**ISO/IEC 27001:2018 Системи за управление на сигурността на информацията - Изисквания**
	ISO/IEC 27002:2018 Кодекс за контроли за сигурността на информацията
	ISO/IEC 27003:2017 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Указания
	ISO/IEC 27004:2016 Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване
	Международна организация по стандартизация и международна електротехническа комисия
	ISO/IEC 27014:2013 Управление на сигурността на информацията
	ISO/IEC TR 27016:2014 Управление на сигурността на информацията – организационна икономика
	ISO/IEC 27032:2012 Насоки за сигурност на информацията
	ISO/IEC 27033-1:2015 Сигурност на мрежи – Част 1: Обща информация и понятия
	ISO/IEC 27033-2:2012 Сигурност на мрежи – Част 2: Насоки за разработване и прилагане на сигурност на мрежи
	ISO/IEC 27033-3:2010 Сигурност на мрежи – Част 3: Референтни мрежови сценарии – заплахи, техники за проектиране и въпроси за контрол
	ISO/IEC 27033-4:2014 Сигурност на мрежи – Част 4: Подсигуряване на комуникациите между мрежи чрез използване на портали за сигурност
	ISO/IEC 27033-5:2013 Сигурност на мрежи – Част 5: Подсигуряване на комуникациите между мрежи чрез използване на VPN мрежи
	ISO/IEC 27033-6:2016 Сигурност на мрежи – Част 6: Подсигуряване на безжичен IP достъп до мрежи
	ISO/IEC 27034-1:2011 Сигурност на приложения – Част 1: Обща информация и понятия
	ISO/IEC 27039:2015 Подбор, изпълнение и работа на IDPS системи
	ISO/IEC 27040:2015 Сигурност на съхранението
	CSA Cloud Controls матрица
	BSI PAS 555:2013 Риск за кибер сигурността. Управление. Спецификация
	PCI Data Security стандарт
	ISF Стандарт за добра практика за сигурност на информацията
	Рамка за политика за сигурност на правителството на Великобритания
	Cyber essentials scheme, правителство на Великобритания
	ETSI GS ISI 001 Част 1: Пълен набор от оперативни показатели за организациите за бенчмаркинг на сигурността
	ETSI TR 103 305 Критични контроли на сигурността за ефективна кибер защита
	BSI 100-1 Системи за управление на сигурността на информацията (ISMS)
	BSI 100-2: IT- Grundschutz методология
	BSI 200-1 Системи за управление на сигурността на информацията (ISMS)
	BSI 200-2: IT- Grundschutz методология
	ISO/IEC 15408-1:2009 Критерии за оценяване за ИТ сигурност – Част 1: Въведение и общ модел
	ISO/IEC 15408-2:2008 Критерии за оценяване за ИТ сигурност – Част 2: Функционални компоненти на сигурността

	ISO/IEC 15408-3:2008 Критерии за оценяване за ИТ сигурност – Част 3: Компоненти за осигуряване на сигурността
	ISO/IEC 19790:2012 Изисквания за сигурност за криптографски модели
	ISO/IEC 27006:2015 Изисквания за органи, предоставящи одит и сертификация на системи за управление сигурността на информацията
	ISO/IEC 27007:2017 Насоки за одит на системи за управление сигурността на информацията
	ISO/IEC 27014:2020 Управление сигурността на информацията
	ISO/IEC 27017:2015: Практически кодекс за контроли на сигурността на информацията, базиран на ISO/IEC 27002 за облачни услуги
	ISO/IEC 29147:2018: Оповестяване на уязвимост
	ISO/IEC 30111:2019: Процеси за управление на уязвимост
	OENORM A 7700-3:201910 Уеб приложения – Част 3: изисквания за сигурност
	ISO/IEC 27701:2019 Техники за сигурност – Допълнение към ISO/IEC 27001 и ISO/IEC 27002 за управление поверителността на информацията. Изисквания и насоки
	ISO/IEC TS 27100:2020 Информационни технологии – Кибер сигурност – Обща информация и понятия

	СТАНДАРТИ ЗА ЗАЩИТА НА ДАННИТЕ И КИБЕР СИГУРНОСТТА
Управление на риска	ISO/TR 31004:2013 Управление на риска – Насоки за прилагане на ISO 31000
	ISO/IEC 27005:2016 Управление на риска за сигурността на информацията
	ISO/IEC 31000 Управление на риска – Техники за оценка на риска
	IEC 31010:2009 Управление на риска – Техники за оценка на риска
	BSI BIP 0076 Управление на риска за сигурността на информацията. Наръчник за ISO/IEC 27001
	BSI 100-3: Анализ на риска на базата на ИТ-Grundschutz
	BSI 200-3: Анализ на риска на базата на ИТ-Grundschutz
	ISO/IEC 27005:2018 Управление на риска за сигурността на информацията
	ISO/IEC 27102:2019 Управление на сигурността на информацията — Насоки за кибер застраховка

	СТАНДАРТИ ЗА ЗАЩИТА НА ДАННИТЕ И КИБЕР СИГУРНОСТТА
Управление на непрекъснатост на дейността	ISO 22301:2012 Системи за управление на непрекъснатост на дейността – Изисквания
	ISO 22313:2012 Системи за управление на непрекъснатост на дейността – Насоки
	ISO/IEC 27031:2011 Насоки за готовност на ИКТ за непрекъснатост на дейността
	100-4: Управление на непрекъснатост на дейността
	OENORM A 7700-4:201910 Уеб приложения – Част 4: Изисквания за сигурни операции

	СТАНДАРТИ ЗА ЗАЩИТА НА ДАННИТЕ И КИБЕР СИГУРНОСТТА
Защита и поверителност на данните	ISO/IEC 27018:2014 Практически кодекс за защита на лична идентифицируемата информация (ЛИИ) в публични облачни услуги, действащи като обработващи ЛИИ
	ISO/IEC 29100:2011 Рамка за поверителност
	ISO/IEC 29101:2013 Рамка за архитектура на поверителност
	BSI BS 10012:2009 Защита на данните. Спецификации за система за управление на лична информация
	CEN CWA 16113:2010 Добри практики за защита на личните данни
	OEVE/OENORM 17529:2020: Защита и поверителност на данните: по избор и по подразбиране
	OENORM A 7700-2:201912 Уеб приложения – Част 2: Изисквания за защита на данните
	ISO/IEC 27018:2019: Практически кодекс за защита на лична идентифицируемата информация (ЛИИ) в публични облачни услуги, действащи като обработващи ЛИИ
	ISO/IEC 29134:2017: Насоки за оценка на влиянието върху поверителността
	ÖNORM EN 419231:2019 11 01: Профил за защита на надеждни системи, поддържащи *time stamping*
	ÖNORM EN 419241-1:2019 03 15: Надеждни системи, поддържащи *Server Signing* - Част 1: Общи изисквания за сигурност на системата
	ÖNORM EN 419241-2:2019 06 01: Надеждни системи, поддържащи *Server Signing* - Част 2: Защитен профил за QSCD за Server Signing

	СТАНДАРТИ ЗА ЗАЩИТА НА ДАННИТЕ И КИБЕР СИГУРНОСТТА
Управление на инциденти	ISO/PAS 22399:2007 Общностна сигурност – Насоки за готовност за инциденти и управление на непрекъснатост на дейността
	ISO/IEC 27036-2:2014 Сигурност на информацията за отношение с доставчици – Част 2: Изисквания
	ISO/IEC 27036-3:2013 Сигурност на информацията за отношение с доставчици – Част 3: Насоки за сигурност на информацията и технологичната верига на доставки
	ISO/IEC 27035-1:2016 Управление на инциденти във връзка със сигурността на информацията – Част 1: Принципи на управлението на инциденти
	ISO/IEC 27035-1:2016 Управление на инциденти във връзка със сигурността на информацията – Част 2: Насоки за планиране и подготовка за реакция при инциденти

	СТАНДАРТИ ЗА ЗАЩИТА НА ДАННИТЕ И КИБЕР СИГУРНОСТТА
Управление на трети страни	ISO/IEC 27036-1:2014 Сигурност на информацията за отношение с доставчици – Част 1: Обща информация и понятия
	ISO/IEC 27035:2011 Управление на инциденти по отношение сигурността на информацията
	ISO/IEC 27037:2012 Насоки за идентифициране, събиране, придобиване и запазване на дигитални доказателства

	СТАНДАРТИ ЗА ЗАЩИТА НА ДАННИТЕ И КИБЕР СИГУРНОСТТА

Индустриална сигурност	OVE EN IEC 62443-4-1:2018 11 01: Сигурност на системи за индустриална автоматизация и контрол – Част 4-1: Изисквания за сигурен цикъл на разработване на продукти
	OVE EN IEC 62443-4-2:2020 01 01: Сигурност на системи за индустриална автоматизация и контрол – Част 4-2: Технически изисквания за сигурност за IACS компоненти
	OVE IEC TS 62351-100-1:2020 06 01