

**МЕТОДИКА
ЗА ОЦЕНКА И ПРОТИВОДЕЙСТВИЕ
НА РИСКА КЪМ
СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ**

1. ВЪВЕДЕНИЕ

Ефективния процес за управление на риска е съществен компонент при изграждането, функционирането и развитието на системите за управление на защитата на личните данни (СУЗЛД)

Основната цел на процесите в организацията, свързани с управлението на риска е защитата на:

- **нейните способности, осигурявани от съответните активи, за изпълнение на бизнес целите и задачите;**
- **обработваните лични данни;**
- **правата и свободите на гражданите, субекти на лични данни (чиито лични данни се обработват в организацията)**

По тази причина (горепосочената основна цел), процесите, свързани с управлението на риска не трябва да бъдат разглеждани единствено и само, като технически въпроси, решавани от специалистите по информационни технологии, опериращи и управляващи съответните системи, а като съществена **управленска функция на Ръководството** на Организацията.

2. ОЦЕНКА НА РИСКА

Оценката на риска е първия процес от методологията за **управление на риска**. Организацията прилага оценката на риска за да определи обхвата на потенциалните заплахи и нивата на риска, свързани с активите, работещи и / или имащи достъп (физически или логически) с / до лични данни

Изхода от този процес е основната предпоставка и критерий за **избор** на защитни механизми, които организацията ще внедри за намаляване или премахване на влиянието на идентифицираните рискове.

Риска е функция от вероятността, даден източник на заплаха да се реализира, чрез конкретна уязвимост (слабост) и от последствията от тази реализация за организацията.

Методологията за оценка на риска включва изпълнението на **9 (девет)** основни стъпки, както следва:

- Стъпка 1 – Определяне на обхвата на СУЗЛД;
- Стъпка 2 – Идентифициране на заплахите;
- Стъпка 3 – Идентифициране на уязвимостите;
- Стъпка 4 – Анализ на защитните механизми;
- Стъпка 5 – Определяне на вероятностите;
- Стъпка 6 – Анализ на влиянието (последствията);
- Стъпка 7 – Определяне на риска;
- Стъпка 8 – Препоръки за защитни механизми за противодействие на разкритите рискове;
- Стъпка 9 – Документация на процеса

Стъпки 2, 3, 4 и 6 могат да се изпълняват съвместно, след като обхвата на СУЗЛД е определен (резултат от стъпка 1)

2.1. Стъпка 1 – Определяне на обхвата на СУЗЛД

Обхвата на СУИС се определя в съответствие с утвърденото за прилагане в организацията “Ръководство за определяне на обхвата на Система за управление на защитата на личните данни (СУЗЛД)” (това Ръководство е налично в материалите към курса за обучение).

Изохода от тази стъпка е документ “Обхват на СУЗЛД”.

2.2. Стъпка 2 – Идентифициране на заплахите

Запахата е възможността, даден източник на заплахата, успешно да използва конкретна уязвимост.

Уязвимостта е слабост, която може да бъде създадена по случаен или умишлен начин.

Даден източник на заплахата не създава риск, ако не съществува уязвимост, която може да използва.

2.2.1 Идентифициране и източниците на заплахи

Целта на тази дейност е да идентифицира потенциалните източници на заплахата, които са **приложими** към активите, работещи с лични данни, определени в документ “Обхват на СУИС”.

Източник на заплахата може да бъде:

- (1) **намерения и методи**, използвани от физическо лице и/ли организация, и насочени към умишлено използване на разкрити уязвимост;
- (2) **ситуация и метод**, който по случаен начин може да създаде уязвимост

Източниците на заплахата се дефинират, като всяко физическо лице, организация, обстоятелство или събитие, предизвикващо вреда на информационните активи, работещи и/или имащи достъп до лични данни..

Общи източници на заплахи са:

Природните бедствия— напр. наводнения, земетресения, буря, земни свличания, атмосферни и електрически аномалии и др. подобни събития.

Хората (персонала - собствен и външен)—напр. събития, които са предизвикани от / чрез поведението на хората - напр. неволни (неумишлени) или умишлени действия.

Промислени аварии в инфраструктурата и замърсявания на околната среда—напр. продължителна повреда в системата за централно електрозахранване, проблеми в комуникационната инфраструктура, замърсявания на атмосферата с вредни вещества, изтичане на вредни химикали и др. подобни събития.

2.2.2 Мотивация и действия за реализация на заплахи

Мотивацията и ресурсите за провеждане на атаки към сигурността на личните данни превръщат **човешкия фактор** в съществен и сериозен източник на заплахи.

Кратко описание на общите заплахи, **произтичащи от хората**, мотивацията за тяхното извършване и методите, и действията за тяхната реализация са показани в следващата таблица (Таблица 2-1). Тази **основна** информация се използва от организацията, като база при изучаването и определянето на конкретните за нея заплахи по сигурността на личните данни, произтичащи от човешкия фактор.

Таблица 2-1 Заплахи от хората: източници, мотивация, и дейности

Източник на заплаха	Мотивация	Действия за реализиране на намеренията
Хакери, кракери	Предизвикателство Самоутвърждаване Недоволство Протест и др.	“Хакинг” Социален инженеринг Проникване, вмъкване в системите Неупълномощен достъп до системите
Компютърни престъпници	Разрушаване на информация Неупълномощено разкриване на информация Спечелване на пари Неупълномощена промяна на данни	Компютърни престъпления Действия за измама Подкупване Измами Проникване в системите
Терористи	Послания (Blackmail) Разрушаване Подготовка на среда и условия за действие Отмъщение	Терористични действия Информационна война Атака на системи Проникване в система Фалшифициране на системи
Индустриален шпионаж (фирми, организации, чужди държави и др.)	Конкурентни преимущества Икономическо разузнаване	Разработване на икономиката Кражби на информация Проникване за придобиване на лични данни Социален инженеринг Проникване в системи Неупълномощен достъп до системите
Служители на организацията (напр. лошо обучени, недоволни, злонамерени, небрежни, нечестни или уволнени)	Любопитство Самоутвърждаване Разузнаване Спечелване на пари Отмъщение Неволни грешки и пропуски	Нападение срещу служители Послания Търсене на определена информация Злоупотреба с компютрите Измами и кражби Подкупване Въвеждане на фалшифицирани Прихващане, подслушване Въвеждане на зловредни програми Продажба / разкриване на персонални данни Проникване в системите Саботаж на системите Неупълномощен достъп до системите

2.2.3 Списък на идентифицираните заплахи

Списъкът на идентифицираните заплахи се създава на база експертна оценка на възможните за реализация заплахи към активите на организацията, работещи с лични данни, без да се отчитат на този етап изградените и/или планирани за внедряване контроли / защитни механизми.

В Таблица 2-2 е показана информация, **подпомагаща** определянето на приложимите заплахи за организацията (за нейните активи, работещи с лични данни).

На базата на Таблица 2-2 се разработва и документа “**Списък на идентифицираните заплахи**” – изход от работата по тази стъпка

Таблица 2-2 Заплахи – видове, мотивация и приложимост

№	Вид на заплахата (кратко описание)	Уязвимости за реализация на заплахата	Мотивация за реализация на заплахата	Приложимост на заплахата (отчита се в СУЗЛД)
1	<p align="center">ЗАПЛАХИ, ПРОИЗТИЧАЩИ ОТ ОБКРЪЖАВАЩАТА СРЕДА</p> <p>Тези заплахи включват природни бедствия и други състояния на околната среда. Резултатите от реализирането на тези заплахи са свързани със загуба на <u>наличност на личните данни</u> и могат да доведат до:</p> <ul style="list-style-type: none"> - Вземането на погрешни управленски решения; - Невъзможност за изпълнение на важни за бизнеса задачи; - Загуба на репутация; - Финансови загуби; - Юридически отговорности ; - Нарушаване на правото на гражданите за защита на личните им данни; <p>В допълнение, тези заплахи могат да засегнат и здравето на персонала. Ако към тези заплахи се прибави и слаба физическа</p>			

	сигурност, то резултатите могат да предизвикат <u>загуба и на</u> <u>конфиденциалност на личните данни</u>			
1.1	Природни бедствия			
	- Земетресение	- Местоположението на организацията е в земетръсна зона - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи - Липса на "back-up" файлове и системи	неприложимо	
	- Пожар	- Местоположението на организацията е в пожароопасна зона - Липса на техническа пожароизвестителна система - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи - Липса на "back-up" файлове и системи	неприложимо	
	- Наводнение	- Местоположението на организацията е в район, застрашен от наводнения - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи - Липса на "back-up" файлове и системи	неприложимо	
	- Буря	- Местоположението на организацията е в район, застрашен от поява на силни бури - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи	неприложимо	

		- Липса на "back-up" файлове и системи		
1.2	Състояние на околната среда			
	- Замърсяване – дим от пожари (външни и в сгради), запрашаване, почистващи химикали, биологически, химически или ядрени реагенти.	- Местоположението на организацията е в район, застрашен от замърсявания - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи - Липса на "back-up" файлове и системи	неприложимо	
	- Електромагнитни излъчвания – сигнали от източници на радиочестотни излъчвания и тяхната интерференция с компютърното оборудване	- Местоположението на организацията е в район, изложен на интензивно радиочестотно излъчване - Липса на екраниращи средства / екранирани помещения - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи - Липса на "back-up" файлове и системи	неприложимо	
	- Екстремни температури и влажност	- Местоположението на организацията е в район, изложен на екстремни температури и влажност - Неадекватно наблюдение на параметри на околната среда - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи - Липса на "back-up" файлове и системи	неприложимо	
	- Аварии в централното електрозахранване	- Липса на система за непрекъсваемо електрическо захранване - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на	неприложимо	

		информационните активи - Липса на "back-up" файлове и системи		
	- Резки / продължителни промени в електрическото напрежение и силата на тока	- Местоположението на организацията е в район, с нестабилни / често променящи се параметри на електрическата мрежа - Липса на система за стабилизиране параметрите на електрическата мрежа - Липса на План за непрекъснатост на бизнеса или Процедури за възстановяване на информационните активи - Липса на "back-up" файлове и системи	неприложимо	
2	<p>ПРЕДНАМЕРЕНИ ЗАПЛАХИ</p> <p>Това са, заплахи, които могат да доведат до преднамерено разрушаване или манипулация на информационните активи и личните данни с които работят..</p> <p>Основния източник и на такъв тип заплахи са хората – напр. недоволни служители или контрагенти, консултанти, хакери, персонал за поддръжка и обслужване, потребители, доставчици, терористи, престъпници, разузнавачи и др.</p> <p>Резултатите от реализацията на тези заплахи могат да доведат до загуби на <u>наличност, конфиденциалност и цялостност на личните данни</u> и последствия за организацията, свързани с:</p> <ul style="list-style-type: none"> - Финансови загуби; - Загуба на репутация; 			

	<ul style="list-style-type: none"> - Вземане на лоши и/или необосновани решения; - Юридически за отговорности; - Неудобства за обществото; -Прекъсване изпълнението на договорирани задължения; - Нарушаване на правото на гражданите за защита на личните им данни; - Юридически за отговорности; 			
	<ul style="list-style-type: none"> - Отказ на обслужване на заявки за изпълнение на услуги – атаки/действия за разрушаване на обслужването на легитимните клиенти , мрежи, системи и ресурси 	<ul style="list-style-type: none"> - Липса на Firewall; - Неадекватно управление на комуникационните мрежи (гъвкавост на маршрутизирането); - Използване на стари версии на операционни системи, слабостите на които са премахнати в по-новите версии; - Липса на използване на публикувани актуални данни и информация, от водещи организации по сигурността, свързани с разкрити нови уязвимости на системите; 		
	<ul style="list-style-type: none"> - Прослушване – “прослушване” на целия трафик, преминаващ през вътрешни и външни мрежи 	<ul style="list-style-type: none"> - Некриптирани комуникации; - Липса на мерки за физическа сигурност на шкафове, съдържащи комуникационно оборудване; - Използване на технологии за разпространяване на целия трафик до всички компютри от даден локален мрежови сегмент (напр. Shared Ethernet) 		
	<ul style="list-style-type: none"> - Пожар – преднамерено предизвикан в 	<ul style="list-style-type: none"> - Липса на мерки за физическа сигурност; 		

	сграда / помещение на организацията	<ul style="list-style-type: none"> - Липса на техническа пожароизвестителна система; - Липса на автоматична система за загасяване на пожар; - Небезопасени, лесно запалими материали; 		
	- Злонамерен код – “вируси”, “Троянски коне”, “червеи”, “шпионски средства” и др.	<ul style="list-style-type: none"> - Липса на антивирусен софтуер; - Липса на периодична подмяна на антивирусен софтуер; - Липса на адекватно обучение на персонала по въпросите на “вирусите”; - Неконтролирано извличане и употреба на софтуер от Интернет; - Липса на Политика за отваряне на приложения в електронната поща; - Липса на контрол на “instant messaging” - Липса на контрол за използване на неразрешен софтуер; - Липса на Политика за използване на преносими средства за съхранение на данни (преди да са сканирани с антивирусен софтуер) 		
	- Злонамерена подмяна/промяна на данни, информация	<ul style="list-style-type: none"> - Липса на мерки за физическа сигурност; - Липса на Система за логически контрол на достъпа (потребителска идентификация и пароли); - Липса на комуникации между отделите за личен състав и ИТ, относно обмен на съответната информация за своевременно отнемане на правата за достъп на напуснали / уволнени служители 		
	- Подмяна на идентичност	- Липса на механизми за идентификация и		

		автентикация; - Незащитени списъци / таблици с пароли; - Липса на механизми за идентифициране на податели и получатели		
	- Отхвърляне на съгласувани пълномощия за определени транзакции	- Липса на доказателства за предаване и получаване на съобщения; - Липса на система за електронен подпис		
	- Саботаж	- Липса на физическа сигурност - Липса на логически контрол на достъпа - Липса на система за управление на конфигурациите - Некоректно предоставени права за достъп - Осигурен достъп до големи масиви на информация на персонал, нямащ необходимост да е познава		
	- Социален инженеринг	- Липса на познания в персонала за заплахите и техниките за провеждане на социален инженеринг - Липса на политика, ограничаваща предоставянето на информация по телефон - Липса на политика за отказ на даване на информация към лица, преди да е установена надеждно тяхната самоличност		
	- Измами и кражби	- Липса на физическа сигурност - Липса на приложни защити срещу извършване на измамни плащания - Липса на процедурни защити срещу извършване на измамни плащания - Липса на автентикация, водещо до приемане на невярна информация, предоставена от		

		<p>неустановени лица/организации</p> <ul style="list-style-type: none"> - Липса на логически контрол на достъпа, водещ до нарушаване на конфиденциалността и възможност за последващи измами - Липса на управление на конфигурациите на софтуер, водещо до възможност за последващи измами - Липса на контрол и проверки за наличност на непозволен софтуер - Липса на контрол на изходящ трафик - Неконтролирано размножаване на данни и софтуер 		
	- Неупълномощен достъп до данни	<ul style="list-style-type: none"> - Липса на логически контрол на достъпа - Невъзможност за автентикация на заявител за достъп до информация - Липса на защита на вход/изход за безжична комуникация - Лоши политики и/или процедури за управление, обработка и съхраняване на информацията - Липса на криптографски средства при предаване на важна информация и/ли данни - Липса на физическа сигурност на комуникационни шкафове и оборудване - Съхраняване на некриптирани важни данни и/или информация на мобилни устройства / компютри 		
	- Неупълномощен отдалечен достъп	<ul style="list-style-type: none"> - Липса на одитиране на логове с цел разкриване на неупълномощен достъп - Липса на автентикация на потребителите 		

		<ul style="list-style-type: none"> - Липса на firewall - Липса на ограничаване на по време на достъпа на потребителите - Липса на физическа сигурност на телекомуникационното оборудване, разположено извън сградите и помещенията на организацията 		
	- Неупълномощени промени на софтуер	<ul style="list-style-type: none"> - Липса на политики и процедури за управление на конфигурациите - Липса на специализиран софтуер за управление на конфигурациите - Лошо разпределение на задълженията между разработчиците на софтуер и останалия персонал - Лош процес за софтуер – инженеринг - Лош процес по качеството на софтуера, свързан с провеждането на периодични прегледи на разработването и програмирането - Лош процес на наблюдение и контрол върху разработчиците на софтуер - Лоша организация на докладването за слабости при работата на софтуерни продукти - Липса на backups 		
	- Употреба на “пиратски” (нелицензиран) софтуер	<ul style="list-style-type: none"> - Липса на политика за ограничаване на използването на нелицензиран софтуер - Лошо управление на разпространението на софтуер - Липса на одити по софтуера – инсталиран, лицензиран, нелицензиран, необходим, инсталиран без необходимост и др. 		

		- Липса на управление на копирането на софтуер		
	- Проникване във WEB Site	- Липса на софтуер за разкриване на прониквания - Липса на firewall - Лоши или липса на политики за firewall - Липса на обновяване на операционните системи – свързани с подобрения по сигурността (security patches)		
3	<p>СЛУЧАЙНИ (НЕПРЕДНАМЕРЕНИ) ЗАПЛАХИ</p> <p>Този тип заплахи, обикновено са свързани с грешки и/или пропуски. Грешките и пропуските, извършени от служителите на организацията са един от основните източници на проблеми с информационната сигурност, вкл. И със сигурността на личните данни.</p> <p>В не малко случаи грешките могат да бъдат сериозна заплаха (напр. програмни грешки, водещи до “сриване” на система) или да създадат уязвимост (напр. оставен без наблюдение екран, съдържащ важна информация, може да бъде прочетена от лице, нямащо необходимост да е знае)</p> <p>Този тип заплахи може да доведе до:</p> <ul style="list-style-type: none"> - Вземането на некоректни решения от бизнеса - Разрушаване на бизнес процеси и 			

	<p>функции</p> <ul style="list-style-type: none"> - Загуба на репутация пред клиентите и партньорите - Невъзможност за изпълнение на задължения по договори - Непредвидени финансови разходи - Нарушаване на правото на гражданите за защита на личните им данни; 			
	<ul style="list-style-type: none"> - пожар в сгради и/или помещения 	<ul style="list-style-type: none"> - Местоположение в район в висока степен на риск от възникване на пожари - Лош физически контрол на достъпа до сгради и помещения - Липса на пожароизвестителна система - Липса на автоматична противопожарна система (вкл. за загасяване на възникнал пожар) - Липса на план за действие при възникване на пожар - Липса на план за възстановяване на информационните активи, засегнати от пожар - Липса на back-up файлове или системи 		
	<ul style="list-style-type: none"> - отпадане на комуникациите 	<ul style="list-style-type: none"> - Липса на резервиране - Лоша система за управление на мрежите - Липса на планове за комуникационната инфраструктура - Лошо управление при възникване на инциденти 		
	<ul style="list-style-type: none"> - отпадане на обслужване от външна страна (outsourcing) 	<ul style="list-style-type: none"> - Лошо описани задължения в договор за външно обслужване - Липса на План за непрекъснатост на бизнеса 		

		или процедури за възстановяване на информационните активи - Липса на back-up файлове или системи		
	- загуба или отсъствие на особено важен персонал	- Липса на резервиране на персонала по функции - Липса на документирани процедури за поемане на допълнителни задължения - Липса на план за ред и последователност за приемане на допълнителни задължения и/или функции		
	- погрешно насочване / пренасочване на съобщения	- Лошо обучен персонал - Липса на криптиране на важни данни/информация - Липса на доказателства за получаване на съобщения		
	- грешки на персонала и потребителите	- Лошо обучен персонал - Липса на документация - Липса или лошо организирано управление на конфигурациите - Сложни потребителски интерфейси		
	- софтуерни или грешки при програмиране	- Лоши процедури за разработване на софтуер - Неясни и/или непълни спецификации - Липса или лошо организирано управление на конфигурациите - Недостатъчни програмистки умения в персонала за разработване на софтуер		
	- технически повреди	- Липса на защити от вредни влияния на околната среда - Лошо обучен и трениран персонал - Лоша поддръжка на оборудването		

		<ul style="list-style-type: none"> - Липса на резервиране на помещения - Липса на достатъчен мрежови капацитет, поради лошо планиране и/или поддръжка - Грешки в процеса за управление на конфигурациите - Липса на план и/или процедури за непрекъснатост на бизнеса 		
	- грешки при пренос	<ul style="list-style-type: none"> - Лошо окабеляване - Лошо управление при инциденти - Липса на резервираност - Липса на план и/или процедури за непрекъснатост на бизнеса 		

2.3 Стъпка 3: Идентифициране на уязвимостите

Целта на тази стъпка е да се разработи **Списък на уязвимостите** (недостатъци или слабости) по сигурността, които биха могли да се използват от потенциалните източници на заплахи.

Уязвимост: Недостатък и/или слабост в процедурите, структурата, изграждането, внедряването и/или защитните механизми на активите и системите, които биха могли да бъдат използвани (случайно или преднамерено) и в резултат да се получат пробиви и/или нарушения на политиките за сигурност.

Таблица 2-3 – Уязвимост / Заплаха - взаимовръзка

Пример

Уязвимост	Източник на заплаха	Действие на източника на заплаха
Правомощията на напуснал служител за достъп до информационните ресурси на организацията не са премахнати своевременно	Напуснали служители	Достъп до важни за бизнеса на организацията данни

2.3.1 Източници за разкриване на уязвимости

Техническите и нетехническите уязвимости, свързани с обкръжението на информационните активи на ИТ системи могат да бъдат разкрити чрез различни техники за събиране на съответната информация.

Възможните документиран източници за разкриване на уязвимости включват (но не само):

- Налични документи за извършени оценка и противодействие на риска
- Налични документи за извършени одити по сигурността и препоръките в тях
- Свободно достъпни източници, съдържащи списъци и бази данни за разкрити уязвимости
- Съвети по сигурността от специализирани издания
- Съвети по сигурността на доставчици/разработчици на системен софтуер
- Информация от дейността на специализирани групи за противодействие на инциденти по сигурността (напр. Computer incident/emergency response teams)
- Анализи по сигурността на системен софтуер от различен тип

2.3.2 Тестване на системите

Чрез този активен метод може да се разкрият уязвимостта на активите в системите. Методите за тестване включват използването на:

- Инструментариум за автоматично сканиране за разкриване на уязвимости

- Провеждане на тестове и оценка по сигурността
- Провеждане на тестове за проникване

Резултатите от използването на тези методи спомага за разкриването на уязвимостите по сигурността.

2.3.3 Разработване на списък на изискванията по сигурността

При изпълнението на тази дейност, специалистите, които извършват оценката на риска определят, дали поставените, като условие или разкрити изисквания по сигурността се осигуряват от въведените и/или планирани за въвеждане защитни механизми.

Списъка на изискванията по сигурността включва основните стандарти за сигурност, които могат да се използват систематично за оценка и разкриване на уязвимостите на информационните активи и личните данни с които оперират

Таблица 2-4 описва критериите по сигурността, които могат да се използват за разкриване на уязвимостите за основните области за сигурност

Таблица 2-4 – Критерии за сигурност

Области за сигурност	Критерии по сигурността
Сигурност на управлението	<p>Определяне и възлагане на отговорности</p> <p>Непрекъснатост на поддръжката</p> <p>Способности за отговор при инциденти</p> <p>Периодичен преглед на защитните механизми</p> <p>Персонални пълномощия по сигурността и проучване на персонала</p> <p>Оценка на риска</p> <p>Обучение по сигурността</p> <p>Разделяне на задълженията</p> <p>Планове по сигурността</p> <p>Контрол на издаването / преиздаването / отнемането на пълномощия</p>
Оперативна сигурност	<p>Контрол на замърсявания в атмосферата (прах, дим, химикали и др.)</p> <p>Контрол на качеството на електрозахранването</p> <p>Достъп и разположение на носителите на данни</p> <p>Защита на сгради и помещения (офиси, центрове за данни, компютърни зали и др.)</p> <p>Разпределяне и означаване (маркиране) на данните за външни потребители</p> <p>Контрол на влажност</p> <p>Температурен контрол</p> <p>Работни станции, мобилни компютри, самостоятелно работещи компютри (извън мрежите)</p>

Техническа сигурност	Комуникации (маршрутизатори, системни връзки и др.) Криптография Контрол на достъпа Идентификация и автентификация Разкриване на прониквания в системите Одити на системите
-----------------------------	---

Изхода от тази дейност е разработен **чек – лист** за основните изисквания по сигурността. Този чек – лист или въпросник, може да се използва при определянето на уязвимостите за основните области за сигурност

Изхода от стъпка 3 е разработен Списък на уязвимостите, които биха могли да се използват от потенциални източници на заплаха.

2.4. Стъпка 4: Анализ на защитните механизми

Целта на тази стъпка е да се проведе анализ на внедрените и планираните за внедряване механизми за защита..

2.4.1 Защитни механизми

Защитните механизми могат да бъдат технически и нетехнически. Техническите защитни механизми обикновено се внедряват в хардуера и/или софтуера (напр. механизми за контрол на достъпа, за идентификация и автентикация, за криптиране, разкриване на прониквания и др.) Нетехническите механизми за защита са свързани обикновено с процесите на управление и контрол (напр. политики, процедури, инструкции, ръководства и др., вкл. за персонална и физическа сигурност, и сигурност на обкръжаващата / околната среда).

2.4.2 Категории защитни механизми

Защитните механизми (технически и/или нетехнически) допълнително могат да бъдат класифицирани основно, като **превантивни и разкриващи**.

- **Превантивни защитни механизми** – възпрепятстват опитите за нарушаване на политиките за сигурност и включват защити за контрол на достъпа, криптиране, автентикация и др.

- **Разкриващи защитни механизми** – предупреждават за нарушения и/или опити за нарушения на политиките за сигурност и включват защити, като пътеки за одит, методи за разкриване на прониквания, “чек суми” и др.

2.4.3 Техника за анализ на защитните механизми

Както беше описано в секция 2.3.3, разработването на чек – листа (въпросник) за изискванията по сигурността може да бъде много полезно при анализа на въведените и/или планирани за въвеждане защитни механизми.

Изхода от стъпка 4 е **Списък на текущите и/или планирани за внедряване защитни механизми.**

2.5. Стъпка 5: Определяне на вероятностите

За да се определи общата вероятност, **показваща възможността дадена уязвимост да бъде използвана в среда от свързани заплахи** трябва да се отчитат следните основни фактори:

- мотивация и способности на източника на заплаха
- природата на уязвимостта
- наличност и ефективност на внедрените защитни механизми

Вероятността, с която потенциална уязвимост може да бъде използвана от даден източник на заплаха може да се опише, като висока, средна или ниска

Таблица 2-4 описва тези три нива на вероятност.

Таблица 2-4. Дефиниции на вероятностите

Ниво на вероятност	Дефиниция на вероятност
Високо	Източника на заплаха е силно мотивиран и е с висока степен на способности. Защитните механизми са неефективни.
Средно	Източника на заплаха е достатъчно мотивиран и има необходимите способности. Защитните механизми са налични и могат успешно да затруднят и/или попречат използването на уязвимостта от заплахата.
Ниско	Източника на заплаха няма мотивация и способности. Защитните механизми възпрепятстват или най-малко затрудняват използването на уязвимостта от заплахата.

Изход от стъпка 5 – Градиране на вероятностите – висока, средна и ниска

2.6. Стъпка 6: Анализ на влиянието

Следващата основна стъпка, свързана с определянето на нивата на риска е провеждането на **анализ на неблагоприятното влияние при успешна реализация на заплаха чрез дадена уязвимост.**

Неблагоприятното влияние на дадено събитие по сигурността може да бъде описано, като загуба или нарушаване на едно или на каквато и да е комбинация от конфиденциалността, цялостта и наличността на информацията (личните данни).

Загуба на цялостност - .Цялостност на данните - изисква информацията да бъде защитена от неупълномощена промяна. Когато е извършено неупълномощена промяна на данни (преднамерено или случайно), тогава имаме загуба на цялостност. Ако тази загуба не е коригирана своевременно и надеждно, това може да доведе грешни решения, измами, неточности и др., а също може да е първата стъпка за атака към конфиденциалността и/или наличността на информацията.

Загуба на наличност - Ако се информацията не е налична за ползване от упълномощени потребители, това може да доведе до намаляване на продуктивността на бизнес процесите, или невъзможност за тяхното изпълнение и др.

Загуба на конфиденциалност - Неупълномощения достъп до информацията (преднамерен или случаен) може да доведе до злонамерено разкриване на бизнес данни, персонални данни и др., което да има вредни последствия за организацията, нейните дейности и/или бизнес.

Някои от осезаемите неблагоприятни влияния могат да бъдат измерени количествено чрез загубата на приходи, стойността за възстановяване на системите или с обема усилия, необходими за корекция на проблемите от реализирана заплаха. Други влияния (напр. загуба на репутация и др.) могат единствено да бъдат класифицирани на качествено ниво, като **големи**, **средни** и **малки**.

Таблица 2-5. Дефиниции на размера на влиянието

Размер на влиянието	Дефиниция на влиянието
Голям	Използването на уязвимостта: (1) може да предизвика високо стойностна загуба на основни осезаеми (материални) активи и/или ресурси; (2) може в значителна степен да предизвика нарушаване, вреда или затрудняване на мисия, репутация или интерес на организацията (3) може да предизвика човешки жертви или сериозни наранявания и/или увреждания.
Среден	Използването на уязвимостта: (1) може да предизвика стойностни загуби на осезаеми (материални) активи и/или ресурси; (2) може да предизвика нарушаване, вреда или затрудняване на мисия, репутация или интерес на организацията (3) може да предизвика човешки наранявания и/или увреждания.
Малък	Използването на уязвимостта: (1) може да предизвика загуби на някои осезаеми (материални) активи или ресурси; (2) може да има неблагоприятно влияние върху мисията, репутацията и/или интересите на организацията

Изхода от стъпка 6 е определен размер на неблагоприятното влияние (голям, среден и малък) от реализацията на заплахите.

Забележка: При тази стъпка, при определянето на влиянието, много полезно е ползването на интегрираната оценка на активите, работещи с лични данни, определени в документ „Обхват на УЗЛД“

2.7 Стъпка 7: Определяне на риска

Целта на тази стъпка е да определи нивото на риска. Определянето на риска за всяка обособена двойка **“заплаха – уязвимост”** може да бъде описано, като функция на:

- Вероятността определен източник на заплаха да опита да използва дадена уязвимост
- Размера на неблагоприятното влияние, ако източника на заплаха успешно и използвал дадена уязвимост
- Възможностите на внедрените или планирани за внедряване защити за намаляване или елиминирание на риска

За да се измерва риска е необходимо да се разработят и приложат скала на риска и **матрица за нивата на риск**.

2.7.1 Матрица за нивата на риска

Крайното определяне на риска се получава при умножаването на присвоените коефициенти на вероятността за реализиране на заплаха с тези на неблагоприятното влияние.

На следваща Таблица 2-6 е показано определянето на риска, като голям, среден и малък. В случая е прието, че:

- за висока вероятност се присвоява коефициент 1.0, за средна – 0.5 и за ниска – 0.1
- за голяма влияние се присвоява коефициент 100, за средно – 50 и за малко – 10

Таблица 2-6. Матрица за нивата на риск

Вероятност на заплаха	Малко влияние (10)	Средно влияние (50)	Голямо влияние (100)
Висока (1.0)	Малък риск $10 \times 1.0 = 10$	Среден риск $50 \times 1.0 = 50$	Голям риск $100 \times 1.0 = 100$
Средна (0.5)	Малък риск $10 \times 0.5 = 5$	Среден риск $50 \times 0.5 = 25$	Среден риск $100 \times 0.5 = 50$
Ниска (0.1)	Малък риск $10 \times 0.1 = 1$	Малък риск $50 \times 0.1 = 5$	Малък риск $100 \times 0.1 = 10$

Скала (нива) на риска:

Голям (>50 to 100); Среден (>10 to 50); Малък (1 to 10)

Забележка: присвоените коефициенти на вероятностите и влиянието могат да бъдат и други.

2.7.2 Описание на нивата на риска

Таблица 2-7 описва нивата на риска, определени в Матрицата за нива на риска. Тази скала на риска – **голям, среден и малък** – показва нивото на риск, на което могат да бъдат изложени информационните активи, ако бъде използвана дадена уязвимост от източник на заплаха.

Таблица 2-7. Нива на риска и необходими действия за противодействие

Ниво на риск	Описание на риска и необходими действия
Голямо	Ако е разкрито голямо ниво на риск, съществува голяма необходимост от своевременно прилагане на

	корективни мерки. Дадена съществуваща система може да продължи да функционира, но трябва да се разработи и своевременно приложи План за корективни действия (за противодействие на риска)
Средно	Ако е разкрито средно ниво на риск, прилагането на корективни мерки е необходимо, като също се разработи и План за внедряването на тези мерки в обоснован период от време.
Малко	Ако е разкрито малко ниво на риск, съответното упълномощено лице (организация) трябва да вземе решение дали да се приложат корективни мерки или риска да се приеме.

Изхода от стъпка 7 е определени нива на риска

2.8 Стъпка 8: Препоръки за защитни механизми за противодействие на разкритите рискове

При тази стъпка се разработва предложение за прилагане на избрани защитни механизми, които намаляват нивата на рисковете или елиминират самите рискове (определени в стъпка 7). Основната цел на препоръчаните защитни механизми е, чрез тях, нивата на риск към активите да бъде редуцирано до приемливи за организацията нива. При избора на защитни механизми, препоръчителни за прилагане е необходимо да се отчита:

- ефикасността на предлаганите защити (вкл. оперативната им и техническа съвместимост с изградените информационни системи
- законовата и нормативна уредба, свързана с информационната сигурност
- организационната политика
- влиянието им върху оперативните процеси в организацията
- тяхната степен на защита и устойчивост на работа

Изхода от тази стъпка е **Списък на препоръчаните за оценка и прилагане защитни механизми.**

2.9 Стъпка 9: Документация на процеса

След като оценката на риска е цялостно завършена (идентифицирани са източниците на заплахи и уязвимостите, определени са нивата на риска и са направени препоръки за прилагане на избрани защитни механизми), резултатите от този процес трябва да бъдат описани в специален документ – **Доклад за оценката и противодействието на риска**

Този Доклад е необходим на Ръководството на Организацията за вземането на управленски решения за осигуряване внедряването, оперирането и поддръжката на защитните механизми, с цел намаляване на риска към активите, до приемливи за организацията нива.

Изхода от тази стъпка е **Доклад за оценката и противодействието на риска**, включващ описания на заплахите, уязвимостите, нивата на риск и защитните механизми, подлежащи на внедряване.

3. СОБСТВЕНИЦИ НА РИСКА

За изпълнение на дейностите по управление на рисковете към сигурността на личните данни, Ръководството на Организацията определя длъжностни лица - „собственици на риска”, които, съвместно и под методическото ръководство на Служителя по защитата на личните данни изпълняват основните стъпки от приетата Методология за оценка и противодействие на риска, както следва:

Стъпка №	Наименовани на дейността	Изпълнител
1	Описание на обхвата на СУЗЛД	Служител по защитата на личните данни
2	Идентифициране на заплахите	Собствениците на риска
3	Идентифициране на уязвимостите	Собствениците на риска
4	Анализ на защитните механизми	Служител по защитата на личните данни Собствениците на риска
5	Определяне на вероятностите	Служител по защитата на личните данни
6	Анализ на влиянието (последствията)	Служител по защитата на личните данни Собствениците на риска
7	Определяне на риска	Служител по сигурността на информацията
8	Препоръки за защитни механизми за противодействие на разкритите рискове	Служител по защитата на личните данни Собствениците на риска
9	Документация на процеса	Служител по защитата на личните данни

Забележка:

За да могат да изпълняват дейностите, свързани с управлението на риска, определените **собственици на риска** трябва да са:

- подходящо обучени по въпросите за **анализ и противодействие** на риска;
- на **ръководни позиции в Организацията**, което е гаранция, че познават съответните активи и техните уязвимости, а също, че имат пълномощия за вземане на решения и извършват контрол по изпълнението на изискванията за сигурност на личните данни..

4. ПРИМЕРНИ ШАБЛОНИ ЗА ОПРЕДЕЛЯНЕ НА ОЦЕНКАТА И ПРОТИВОДЕЙСТВИЕТО НА РИСКА

Разработените примерни шаблони са предназначени да **подпомогнат** дейностите за оценка на риска към активите от обхвата на СУЗЛД.

Примерните шаблони са разработени в съответствие с процесите, описани в тази **Методика за оценка и противодействие на риска**

Шаблон № 1 “Оценка на риска за актив”

1. **Тип на актива:** (хардуер, софтуер, данни, документи или персонал – съгласно документ “Обхват на СУЗЛД”)

2. **Описание на актива:** (съгласно документ “Обхват на СУЗЛД”)

3. **Идентификационен № на актива:** (съгласно документ “Обхват на СУЗЛД”)

4. **Идентифицирани заплахи/уязвимости към/на актива:**

№	Описание на заплахата	Описание на уязвимостта	Източник на заплахата	Мотивация на източника на заплахата*	Действия на източника на заплахата, за нейната реализация*
1					
2					
3					
N					

*** Отнася се само за заплахи, чиито източник са хората**

5. Определяне на вероятността за реализация на идентифицирана заплаха

№	Описание на заплахата (1)	Ниво на вероятност за реализация на заплахата (2)	Коефициент на вероятността (3)	Времеви период на вероятността (4)
1				
2				
3				
N				

Забележки:

- (1) Както описанието в т. 4 от този шаблон;
- (2) Въвежда се качествена оценка - високо, средно, ниско ниво;
- (3) Въвежда се коефициент, съответен на качествената оценка – 1(за високо ниво), 0.5 (за средно ниво), 0.1 (за ниско ниво)
- (4) Въвежда се времеви период, за който е отчетено нивото на вероятност за реализация на заплахата – напр. 1 год.

6. Определяне на неблагоприятното влияние при успешна реализация на заплаха чрез дадена уязвимост

№	Описание на заплаха (1)	Описание на уязвимостта (2)	Загуба на конфиденц. (3)	Загуба на наличност (3)	Загуба на цялостност (3)	Размер на влиянието (4)	Коефициент на влиянието (5)
1							
3							
3							
N							

Забележки:

- (1) Както описанието в т. 4 от този шаблон;
- (2) Както описанието в т. 4 от този шаблон;
- (3) Отбелязва се каква загуба (загуби) произтича за информационния актив – да/не за съответния тип загуба;
- (4) Въвежда се качествена оценка - висок, среден, нисък размер на влиянието;
- (5) Въвежда се коефициент, съответен на качествената оценка – 100 (за висок размер), 50 (за среден размер), 10 (за нисък размер)

7. Определяне на нивата на риск към актива

№	Описание на заплата (1)	Описание на уязвимостта (1)	Коефициент на вероятността на заплата (2)	Коефициент на влиянието (3)	Коефициент на нивото на риск (4)	Ниво на риска (5)
1						
2						
3						
N						

Забележки:

- (1) Както описанието в т. 4 от този шаблон;
- (2) Както е определено в т. 5 от този шаблон;
- (3) Както е определено в т. 6 от този шаблон;
- (4) Определя се чрез умножаване на коефициентите за вероятност и влияние на заплата;
- (5) Въвежда се качествена оценка, в съответствие с получения коефициент на ниво на риска – голям (от 50 до 100), среден (от 10 до 50) и малък (от 1 до 10)

Получените стойности за нива на риска към актив, за всяка двойка “заплаха – уязвимост” могат да се разпространят и за други активи (предварително дефинирани групи от активи) от същия тип, имащи:

1. Еднаква или много близка степен на важност;
2. Еднакво или много близко по характеристики физическо обкръжение;
3. Еднакво или в непосредствена близост местоположение
4. Еднакви или много близки по функции и предназначение изградени защитни механизми.

За всеки актив от състава на СУЗЛД, който не може да бъде групиран по избраните общи признаци, всички стъпки (от 1 до 7) се изпълняват индивидуално.

Шаблон № 2 “Регистър на идентифицираните рискове към активите ”

Обобщено представяне на нивата на риска към е активите от обхвата на СУЗЛД – извършва се на база извършените оценки на отделните активи (групи от активи), съгласно стъпките по Шаблон № 1 “Оценка на риска за информационен актив”

№	Актив - идентификационен № / описание	Заплаха	Уязвимост	Последствия – загуба на : (1)	Вероятност на заплахата (коэффициент)	Размер на влиянието (коэффициент)	Ниво на риск (коэффициент)
1		1.	1.	1.	1.	1.	1.
		2.	2.	2.	2.	2.	2.
		М.	М.	М.	М.	М.	М.
2		1.	1.	1.	1.	1.	1.
		2.	2.	2.	2.	2.	2.
		Н.	Н.	Н.	Н.	Н.	Н.
....							
....							
....							
....							

Забележки:

- (1) Въвежда се съгласно идентифицираните загуби в т. 6, Шаблон №1 – “К” за конфиденциалност, “Н” за наличност, “Ц” за цялостност;
- (2) В Регистъра трябва да фигурират всички активи от обхвата на СУЗЛД, независимо, дали оценката на риска за тях е извършвана групово или индивидуално