ДОБРИ ПРАКТИКИ И МОДЕЛИ ЗА ИНФОРМАЦИОННАТА СИГУРНОСТ В БИЗНЕС ОРГАНИЗАЦИИТЕ

Владислав Владимиров Василев
Стопанска академия „Д. А. Ценов“ – Свищов
Катедра „Бизнес информатика“

Резюме: Заплахите пред информационни системи на бизнес организации постоянно еволюират. Намирането на подходящо решение на тези заплахи става изключително трудно поради много допълнителни фактори.

В настоящата статия се обосновава необходимостта от вземане на решение от ръководния състав на бизнес организациите за инвестиции за осигуряване на информационна сигурност. За тази цел са описани и анализирани политики за управление на риска, рамки за неговото оценяване и модели за инвестиции в информационната сигурност. На базата на това са формулирани критерии за избор на модел за инвестиции в системата за информационна сигурност. Отделено е внимание на добрите практики за защита на данните.

Ключови думи: инвестиции в информационна сигурност, управление на риска, оценяване на риска, модели за инвестиции в информационна сигурност, добри практики, критерии за избор.

JEL: M15.

GOOD PRACTICES AND MODELS FOR INFORMATION SECURIY IN BUSINESS ORGANIZATIONS

Vladislav Vladimirov Vasilev
The D. A. Tsenov Academy of Economics – Svishtov
The Department of Business Informatics

Abstract: The threats to information systems of business organizations are constantly evolving. Finding the right solution to these threats is extremely difficult due to many additional factors.

This article justifies the need the management of business organizations to make relevant decisions on investments in information security. To this end, risk management policies, frameworks for risk assessment, and models for investment in information security have been described and analyzed. Based on this, criteria for selecting a model for investments in the information security system are formulated. Attention is paid to good data protection practices.

Keywords: investments in information security, risk management, risk assessment, information security investment models, good practices, selection criteria.

JEL: M15.

Увод

В съвременния свят информационните системи на бизнес организациите са изправени пред предизвикателството да осигурят информационната сигурност на своите дигитални активи от различните видове заплахи.

Практиката показва, че ръководителите на бизнес организациите не отделят нужното внимание на тези изисквания главно поради усилията, насочени към крайния резултат, т.е. печалба и допълнителни дивиденти. Това се дължи на две основни причини:

- Неразбиране и недооценяване на заплахите за пробив на информационната система и загубите, които могат да бъдат причинени в резултат на този пробив;
- Липса на финансова рамка по отношение на информационната сигурност за определяне на необходимите финансови средства за поддържане на нужното ниво на защита. Поради абстрактността на тази материя формулирането на точни параметри е почти невъзможно.

Наред с неразбирането на същността на заплахите и последствията от материализирането им липсата на финансова рамка по отношение на информационната сигурност е една от основните причини, мениджърите на бизнес организациите да не обръщат достатъчно внимание на мерките за подсигуряване и защита на информацията. За съжаление нейното формулиране от ръководителите на фирмите не е лесна задача, тъй като информационната сигурност е абстрактна материя с множество особености.

Настоящата статия има **за цел** да се обоснове необходимостта от вземане на решение за инвестиране в информационна сигурност, да се анализират стъпките на това решение, както и да се опишат възможно най-ясно от гледна точка на мениджмънта на бизнес организацията. Базирайки се на това, може да формулираме като **обект на статията** – информационните активи на бизнес организациите, като **предмет** – тяхната защитата, осигуряване на информационната им сигурност. З**адачите**, които си поставяме са:

1. Описание и анализиране на политики за управление на риска.
2. Описание и анализиране на модели за инвестиции в информационна сигурност.
3. Формулиране на критерии за избор на модел, за инвестиции за създаване на система за информационна сигурност.
4. На базата на формулираните критерии да се предложи използване на един или няколко модела.
5. Представяне на добри практики за защита на данните.

1. Необходимост от защита на информационните активи

С навлизането на новите информационни технологии настъпват значителни промени в различните сфери на човешката дейност. Тези про-

мени не само оказват влияние върху организационната структура, но и подпомагат начините за извършване на различни дейности на цели отрасли. Важна роля в тази промяна има дигиталната информация и превръщането ѝ в стратегически ресурс, използван в различни сфери. Всяка една бизнес организация се стреми да използва своята информационна система за ефективно обработване на събраните данни и тяхното съхраняване. Но едновременно с това се увеличават заплахите, насочени към информационната сигурност. Според доклада на Симантек (Symantec Yearly Internet Security Threat Report, 2017) броят на заплахи в интернет пространството към април 2017 г. показва, че изминалата година е била много динамична по отношение на заплахите за сигурността. Като се започне от дигиталния обир на банка в Бангладеш, откъдето са откраднати над 81 милиона долара, и се премине към най-големите досега атаки от тип отказ от услуги към бизнес организации, държавни структури и инфраструктура. В посочения доклад също така се обръща внимание на изобретателността на киберпрестъпниците, която се проявява в старите типове заплахи тип – спам, подслушване на трафика и др. Голяма част от тях проявяват изключителна креативност в атаките си, симулирайки истински сайтове с изключителна точност – това са сайтовете на Epay.bg, Paypal, НАП и др.

Друг сериозен проблем, който се появява, е формирането на връзки на киберпрестъпници с реалния престъпен свят, като синхронизирането на действията между двете групи са изключително притеснителни. Не на последно място от Симантек докладват и за увеличаващата се опасност от криптовируси и огромните на брой атаки извършени от тях.

Необходимо е също така да се обърне внимание на увеличаващите се заплахи от използване на различни видове зловреден софтуер и атаки от типа на отказ от услуга в много по-голям от обикновения мащаб, които прерастват в геополитически сблъсъци.

На базата на представената по-горе информация следва да се повдигне въпросът дали ръководителите на бизнес организациите имат дефинирани политики, направена правилна оценка на риска за информационните си активи и необходимите ресурси за ефективна защита на информацията. Заплахите са постоянно еволюиращи и това е обстоятелството, което изисква навременен отговор за намаляване на риска от пробив. С описание на добрите практики за управление на риска и рамки за неговото оценяване, анализиране на различни модели за инвестиции в информационна сигурност правим опит да дефинираме необходимите стъпки за изграждане на ефективна защита на информацията.

2. Управление на риска за сигурността на информационната система

Добрите практики за управление на риска са важна част от изграждането на ефективна система за информационна сигурност. Те помагат за балансиране на икономическата ефективност на защитата на

информационните активи на бизнес организацията. В тази насока има различни варианти, като най-често срещаните са базирани на ISO27001 и са сертифицирани по този стандарт. Колдър и Уаткинс (Calde & Watkins, 2010) описват стандартите на ISO/IEC 27002:2005, които са сред най-добрите практики за управление на риска. Според тях е необходимо на първо място да се дефинира подходът за оценка на информационните активи и след това да се анализира рискът от потенциалните загуби. Последната актуализация на този стандарт е от 2013 г., с която се предоставят допълнителни възможности за управлението на риска и оценката му. Използването на ISO/IEC 27002:2013 се препоръчва да се прилага в случаи, когато ще се изисква сертификация по този стандарт. Но практиката налага да се използват и по-различни подходи.

Подобно мнение имат Стоунбърн, Гогуен и Феринга (Stoneburne, Goguen, & Feringa, July 2002), посочвайки, че ръководството на бизнес организацията трябва да бъде много добре осведомено, без да се навлиза в специфични документи и/или обяснения на международни стандарти. Те представят опростен модел, състоящ се от няколко фази за инвестиция в система за информационна сигурност:

- Начало – откриват се рисковете и на тяхна база се създава стратегия за сигурност;
- Придобиване или разработка на система за информационна сигурност – откритите рискове се използват за създаването на архитектура за защита на информацията;
- Осъществяване – включва самия процес за осъществяване на зададените изисквания;
- Поддръжка – поддържане и експлоатация;
- Премахване – премахване, замяна на информация, хардуер и софтуер.

Рамка за оценяване на риска за сигурността и надеждността на информацията е предложена от Киси, Люидонг и Уанг (Qisi, Liudong, & Wang, 2017). При оценяването на риска авторите разглеждат в подробности заплахите за сървърите и облачното пространство. Те използват триъгълника конфиденциалност, цялостност, достъпност като основа за анализиране на възможността за риск от инциденти. В своето изследване авторите описват как се противодейства ефективно на заплахи, подчертавайки, че подобряването на информационната сигурност увеличава едновременно с това и надеждността.

Други автори като Майадун и Парк (Mayadunne & Park, 2016) обръщат внимание на желанието на висшия мениджмънт на бизнес организациите за поемане на риск. Те посочват, че поемащите риск отделят повече средства за защита, базирайки се на потенциалните уязвимости на набора от информационни активи, а не на стойността им. Докато при нежелаещите да поемат риск се наблюдава извършване на по-малки инвестиции за изграждане на система за информационна сигурност.

3. Модели за инвестиции в информационната сигурност

Управлението на риска и неговото оценяване са важни насоки от решението за инвестиции в информационната сигурност, но като част от това решение е важно да се изяснят финансовите параметри на този процес. Дори когато има сериозни заплахи за информационната сигурност, трудно се взема решение за инвестиции за нейното осигуряване. Обикновено ръководните отдели не отдават нужния приоритет на инвестициите в информационна сигурност дори и при направена оценка на такъв риск, поради абстрактността на тази тематика. Техните очаквания са, че срещу инвестиция се очаква възвръщаемост на вложения ресурс, а това при информационната сигурност не стои така.

За подпомагане вземането на решение за инвестиране в информационна сигурност може да се използват специално дефинирани модели за оценка на необходимите инвестиции. Те представят различни подходи за оптимално инвестиране в информационна сигурност. По-долу са представени моделите за инвестиране на Гордон-Лоеб – ориентиран към смекчаване на щетите; на Соненрич – ориентиран към определянето на риска за пробив; на Креморини и Мартини – ориентиран към определяне риска на базата на годишни отчети; на Боджанк, Блазис и Текавкик – модел за оценяване на риска.

Модел на Гордон и Лоеб

Този модел е разработен от Гордън и Лоеб (Lawrence & Loeb, 2002). Тяхната идея е да се направят инвестиции за осигуряване на информационната сигурност за смекчаване на щетите от вече съществуваща уязвимост. Това означава, че не трябва да се фокусира върху потенциалната загуба или уязвимост в информационната система на бизнес организацията, а да се обърне внимание на уязвимостите със средно ниво на риск.

Моделът се базира на следните предположения:

- Ако информацията е напълно откъсната, има регулиран достъп до нея, тя ще остане напълно защитена и няма да има нужда от инвестиции в информационната сигурност;
- Ако няма инвестиции в информационната сигурност и има външен достъп до информацията, то вероятността за нарушаване на сигурността зависи от ценността на съхраняваната информация;
- С увеличаването на инвестициите в сигурността, информацията става по-сигурна, но с отслабваща защита в дълъг времеви период;
- Чрез достатъчно инвестиране в сигурността вероятността за нарушение на сигурността се свежда до практическа нула.

Когато дадена информация е добре защитена, било чрез криптиране, отдалечен достъп с определен ключ, оторизиране на потребители с необходимите права, тя е сигурно защитена дори и когато не се инвестира

в средства за нейната защита. Но също така Гордон и Лоеб отбелязват, че в информационните технологии няма константи, технологиите се развиват – криптирането се усъвършенства като алгоритъм, но ако останат без актуализация и поддръжка, защитата им лесно ще бъде преодоляна. Това налага постоянно внимание и инвестиране за намаляване на риска от пробиви в сигурността. Но дори и да се инвестира регулярно, самата защита като стойност е намаляваща във времето. Гордон и Лоеб изчисляват, че оптимално трябва да се влагат не повече от 37 % от очакваната загуба на базата на направен или хипотетичен пробив.

На базата на това са определени със сравнителна точност параметри, които може да помогнат за създаването на точен бюджет, свързан с вземането на решение за инвестиция в информационна сигурност. Този модел се фокусира върху базовите правила за защита и калкулира с препоръчителни параметри базова финансова рамка.

Следва да отбележим, че моделът на Гордон и Лоеб се допълва с **допълнителни проучвания**, заедно с други автори Лусушун и Жоу (Lawrence, Martin, Lucyshyn, & Zhou, 2015), но концепцията остава същата, в нея се наблюдават малки изменения.

В посоченото научно изследване авторите обръщат внимание на случаите, при които се пренебрегва информационната сигурност от малки, средни и големи предприятия и организации. Също така те акцентират на желанието за поемане на риск и отговорността, вървяща с него. На базата на това считаме, че е съществена връзката между оценяването на риска от пробив и поемането на отговорността за риск при изготвянето на финансов план за инвестиция и изпълнението му. Според тези автори това са базовите стъпки за изграждане на ефективна защита.

Модел на Соненрич

Според Соненрич, Албанезе и Стоут (Sonnenreich, Albanese, & Stout, 2006) възвръщаемостта на инвестицията се определя на базата на риска от пробив, смекчаване на евентуалната загуба и разходите за тях. Авторите обръщат внимание, че определянето на риска и неговото смекчаване е изключително трудно, защото няма нито един модел или подход, който да дава точни резултати. Като допълнителни параметри за намаляване на тези трудности те предлагат следните критерии:

- Към измерване на риска – задълбочено изследване по отношение на връзката оценяване на риск с продуктивността на организацията;
- Към смекчаването на загубата – използването на различни алгоритми и сравняване на техните резултати;
- Към разходите – трябва да се определи въздействието на използваните ресурси върху продуктивността на работата на организацията.

С включването на тези допълнителни параметри цитираните по-горе автори предлагат възможност за по-добро разбиране на „риска“ и

неговото влияние върху други фактори. На базата на това може да се предположи, че продуктивността е важен фактор, който може да бъде повлиян от подобряването на нивото на сигурност.

Този модел е свързан също и с началните стадии за управление на риска и макар да е насочен към една определена рамка, позволява по-голяма свобода при имплементиране на информационна сигурност. Авторите считат, че още при вземането на управленско решение за инвестиции в информационна сигурност може да се предприемат нужните контрамерки, но те подлежат и на допълнителни изменения в зависимост от влиянието си върху работа на бизнес организацията. Това може да бъде представено като определена рамка с възможни функции за смекчаване на загубите, но не предвижда и няма изградено противодействие при постоянно еволюиране на заплахите.

Модел на Креморини и Мартини

В своя модел Креморини и Мартини (Cremonini & Martini, 2005) калкулират възвръщаемостта на инвестициите в информационната сигурност на базата на годишните прогнози за загуби. Те представят аргумента, че базирайки се на един индекс за оценка на информационна сигурност, се очертава само частично характеризиране. Креморини и Мартини дефинират и добавят като допълнителен индекс – възвръщаемостта на инвестициите след успешна атака, свързан с типа на зловредната атака и начините за нейното противодействие.

Това включва **постоянството,** с което се извършват опитите за пробив в информационната сигурност и как се противопоставят на тези опити имплементираните контроли за сигурност. Те отбелязват, че възвръщаемостта на инвестициите след успешна атака спомага и за определяне на приспособяването на средата към промените, които се налагат с приведеното в действие решение за осигуряване на информационна сигурност. Креморини и Мартини отбелязват, че индексът им не може да определи с точност тези промени. Те допускат допълнително анализиране, насочено към връзките между подобряването на нивото на сигурността и производителността на бизнес организацията.

Този модел показва, че съществува връзка към предварително зададени финансови параметри като очакваната загуба. Изследването на вида заплаха, с която е извършена атака, може да бъде използвано за определяне на следващите потенциални загуби. Нашето мнение е, че моделът е рисков за използване поради приемането на всяка потенциална атака. Рядко бизнес организации биха се изложили на такъв продължителен анализ за подобряване на сигурността.

Моделът на Боджанк, Блазис и Текавкик

Боджанк, Блазис и Текавкик (Bojanc, Jerman-Blazic, & Tekavcic, 2012) акцентират на представянето на математически модел за оптимално инвестиране в информационната сигурност и процеса за вземането на решения за инвестиции, базирайки се на задълбочено изследване на риска за информационните активи на бизнес организацията. Според тях трябва

да се обърне внимание на видовете мерки за информационна сигурност и влиянието им върху функционалността на организацията. Едновременно с това те представят и необходимостта за дефиниране на ясна и точна методология за контролиране на риска. Техният модел се формира от:

- Оценка на информационните активи;
- Степента на уязвимост на системата;
- Вероятността за пробив;
- Загуби след извършен пробив.

Към опитите за намиране на потенциалните загуби чрез финансова рамка Боджанк, Блазис и Текавкик предлагат и опростена система за определяне на риск, базираща се на следните правила:

- Редуциране на риска;
- Предаването на риска;
- Приемането на риска.

Те предлагат и опростени правила за изграждане на информационната сигурност:

- Мерки за превенция – редуциращи възможността за пробив;
- Мерки за корекция/редуциране – редуциране на загубата;
- Мерки за идентификация – начини за навременно сигнализиране за нередности.

На базата на представеното по-горе стигаме до заключението, че този модел предлага систематизирано анализиране и управление на риска, начин за инвестиция в информационна сигурност и политики, базирани на добрите практики.

Според нас този модел е алтернатива на използването на по-комплексни методологии и стандарти, съсредоточавайки се в извеждането на точни параметри и поставяне на акцент върху уязвимостите на използваните информационни системи. Но трябва да се обърне внимание, че защита на информационните активи се определя според оценката на риска им за информационната сигурност на бизнес организацията. При инвестиции в информационна сигурност не се обръща внимание на подобрения, а на поддържане на системите.

4. Критерии за избор на модел за инвестиция от гледна точка на бизнес организацията

След представянето на избраните модели за инвестиции за осигуряване на информационна сигурност ще дефинираме критерии за тяхната приложимост от гледна точка на бизнес организациите. Нашето предложение е:

- Финансова рамка – използването на финансовите ресурси;
- Начин на инвестиция;
- Ползи;
- Негативи.

Таблица 1
Сравнение на моделите за инвестиции за осигуряване на информационна сигурност

Критерии	Модел на Гордон-Лоеб	Модел на Соненрич	Модел на Кремо-рини и Мартини	Модел на Боджанк, Блазис и Текавкик
Финансова рамка	Представя се оптимална инвестиция от 37 % от нетните при-ходи.	Представя се финансова рамка, която се базира на цен-ността на ин-формацията и не може да се опре-дели с точност.	Представя се рамка, базирана на годишен фи-нансов план, предвиждайки потенциални загуби проме-няща се на база на атаките.	Представя се финансова рамка, която се базира на ценността на информацията и уязвимостта на системата.
Начин за инвестиция	Фиксиран начин за инвестиция с точни и ясно дефинирани параметри.	Фиксиран начин за инвестиция, който се опре-деля още в на-чалния стадий за изграждане на информационна сигурност.	Фиксиран начин за инвестиция, базирайки се на годишните очак-вания от загуби и възвръщаемостта на инвестициите след успешна атака.	Фиксиран, пред-лагащ възмож-ност за продъл-жителна инвес-тиция, базирайки се на анализите за риска на ин-формационните активи.
Ползи	Ползите се изразяват в защита на активите с по-голям риск за при-чиняване на вреда и изг-раждане на защита за тях с фиксиран размер на инвестиция.	Моделът пред-лага ползи, ак-центирайки вниманието към смекчаването на загубите и отбе-лязване на връз-ката между продуктивността и сигурността на бизнес органи-зацията.	Моделът пред-лага анализ на атаките, които постоянно заст-рашават сигур-ността на ин-формацията.	Ползите произ-лизат от дефи-ниране и оце-няване на риска и предло-жените политики за информаци-онна сигурност, базирани на добри практики.
Негативи	Не се обръща внимание при малка веро-ятност за пробив, от което се възползват атакуващите.	Не се вземат под внимание посто-янно еволюира-щите заплахи. При такава въз-можност и смекчаването на загубите може да не е ефек-тивно.	Постоянното излагане на риск от пробив може да бъде нерента-билно и потенци-ално опасно.	Възможността за претърпяване на промени при определянето на финансовите параметри, бази-райки се на ана-лизирането и оценяването на риска.

На основата на направения анализ предлагаме да се използват положителните страни на модела на Гордон и Лоеб – по-точно фиксираните стойности за инвестиция и ползите от определяне и оценяване на

рисковете предложени от модела на Боджанк, Блазис и Текавкик. Това би помогнало в изграждане на ефективна система за информационна сигурност.

5. Добри практики и решения за защита на данните

За да бъде осигурено допълнително ниво на защита, предлагаме да се разгледат някои добри практики и решения, които могат да бъдат взети под внимание при вземането на решение за инвестиции в информационната сигурност.

Въпреки че управлението на риска и неговата оценка са основните компоненти за вземане на решение за инвестиции в информационната сигурност, трябва да се обърне внимание и на първоизточника на защитаваната информация. Това се постига чрез анализ на източниците на информация. За тази цел предлагаме, те да се разгледат в следните аспекти:

- Идентифициране на източниците, които ще се използват – необходимо е да се определят точно кои източници ще се използват за събиране на необходимата информация, кой е първоизточникът и дали е надежден;
- Как ще се събира информацията – трябва да се дефинира вида на събираната информация, отговаряща на нуждите на организацията. Това е сложна задача, защото трябва да се вземат предвид индустриалните стандартите и законите на съответната страна;
- Къде ще се складира информацията – избиране на подходящия склад за данни и базата от данни. Необходимо е да се прецени къде те ще бъдат разположени в самата организация или извън нея;
- Контрол – като добра практика контролът трябва да бъде осъществяван върху процесите по идентифициране, събиране и складиране на данните.

От гледна точка на осигуряване на информационната сигурност Нджила, Камхоуа, Куаиат, Хърли и Писиноу (Njilla, Kamhoua, Kwiat, Hurley, & Pissinou, 2017) предлагат модел за защита, която е многослойна. Нивата, които те предлагат са :

- Атака;
- Избягване;
- Предотвратяване;
- Откриване;
- Оцеляване;
- Възстановяване.

Като част от процеса за вземане на решение за инвестиции в информационна сигурност трябва да се анализира самата информационна инфраструктура. Инфраструктурата в повечето случаи представлява едно

централно сървърно помещение и прилежащите му. Тази архитектура също така може да бъде изведена в облачно пространство. Облачното пространство предоставя възможност за връзка и контрол от специализирани устройства до терминали/работни станции, както и връзка тип VPN за достъп. В подкрепа на това решение Ченгао, Кси, Жанксианг и Тиан (Chenghao, Xi, Zhanxiang, & Tian, 2010) предлагат изграждане на цялостна информационна инфраструктура в облачното пространство. Предимствата на това решение са възможността за контролиран достъп и улесненатa администрация, като едновременно с това отговорността за осигуряване на информационна сигурност се прехвърля на друг.

Намаляването на щетите и определянето на финансовите параметри са описани от Бенерок (Benaroch, 2017)**.** Той отделя внимание на прилагането на практики от частни фирми, главно на една Японска компания. Тези практики са насочени към ефективна защита и намаляване на щетите. Намаляването на щетите може да бъде сегментирано в няколко направления в зависимост от ценността на информацията:

- Предотвратяваща;
- Справяща се;
- Учаща се.

Заключение

На базата на изложеното по-горе стигаме до заключението че контролът на риска и неговият анализ са изключително важна част от решението за изграждане на информационната сигурност. То е основополагаща стъпка, която бизнес организациите трябва да направят.

Разгледаните модели за инвестиции в информационната сигурност имат различна насоченост, отговаряйки на различните изисквания на мениджмънта. Те вземат предвид наличните информационни активи и предлагат различни подходи за осигуряване на тяхната защита.

Предложените от нас критерии обхващат основните акценти към които трябва да се обърне внимание при прилагането на изброените модели за осигуряване на защита. Базирайки се на тях, нашето предложение за използване на полезните страни на моделите осигурява гъвкавост и помага за селекцията на такъв модел и несъмнено ще подпомогне мениджмънта при избора на решение за защита на информационни активи на бизнес организацията.

Използвани източници:

Alan Calder, S. G. (н.д.). *https://books.google.bg/books?hl=bg&lr=&id=8Ffa1dOFgO4C&oi=fnd&pg=PA10&dq=information+security+risk+management&ots=QSWGCRtAdn&sig=5f9VaoZ1YF7Fknkf3RPMT9rGtDE&redir_esc=y#v=onepage&q=information%20security%20risk%20management&f=false*. Изтеглено на 2017 от https://books.google.bg: https://books.google.bg/books?hl=bg&lr=&id=8Ffa1dOFgO4C&oi=fnd&pg=PA10&dq=information+security+risk+management&ots=QSWGCRtAdn&sig=5f9VaoZ1YF7Fknkf3RPMT9rGtDE&redir_esc=y#v=onepage&q=information%20security%20risk%20management&f=false

Benaroch, M. (27 April 2017 r.). *Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision-Making.* Свалено от https://www.ssrn.com/en/: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958894

Bojanc, R., Jerman-Blazic, & Tekavcic, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management*.

Calde, A., & Watkins, S. (2010). *Information Security Risk Management.*

Chenghao, H., Xi, J., Zhanxiang, Z., & Tian, X. (2010). A Cloud Computing Solution for Hospital Information System. *Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on.* Xiamen.

Cremonini, M., & Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). *4th Workshop on the Economics on Information Security 2005.*

Lawrence, G., & Loeb, M. (2002). *ACM Transactions on Information and System Security (TISSEC) - The Economics of Information Security Investment*, 438-457.

Lawrence, G., Martin, L., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, 24-30.

Mayadunne, S., & Park, S. (2016). *International Journal of Production Economics - Economic Model to Evaluate Information Security Investment of risk taking small and medium enterprises*, 519-530.

Njilla, L., Kamhoua, C., Kwiat, K., Hurley, P., & Pissinou, N. (2017). Cyber Security Resource Allocation: A Markov Decision Process Approach.

Qisi, L., Liudong, X., & Wang, C. (2017). Framework of probabilistic risk assessment for security and reliability. *2017 IEEE Second International Conference on Data Science in Cyberspace.*

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return On Security Investment - A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*.

Stoneburne, r. G., Goguen, A., & Feringa, A. (July 2002). *Risk Management Guide for Information Technology Systems.* National Institute of Standards and Technology - United States of America.

Symantec Yearly Internet Security Threat Report. (2017). *Internet Security Threat Report, as of April 2017.*