МРНТИ 10.77.51

Маликова Ш.Б.[1], Омарова А.Б.[2], Маликов Д.Б.[3]

[1] к.ю.н., доцент, e-mail: Sholpan.Malikova@kaznu.kz
[2] к.ю.н., профессор, e-mail: omar_17@mail.ru
[3]преподаватель, e-mail: Dauren.Malikov@kaznu.kz
Казахский национальный университет им. аль-Фараби, Казахстан, г. Алматы

УГОЛОВНАЯ ПОЛИТИКА РЕСПУБЛИКИ КАЗАХСТАН В СФЕРЕ ИНФОРМАТИЗАЦИИ: ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

В настоящей статье исследованы проблемы уголовной политики в сфере обеспечения информационной безопасности, развития уголовного законодательства в этой сфере.

Цель настоящей статьи – исследовать проблемы уголовной политики в сфере информатизации или обеспечения информационной безопасности и теоретических основ противодействия компьютерной преступности. В рамках исследования уточняется понятийный аппарат и теоретические основы уголовной политики в сфере обеспечения информационной безопасности и противодействия компьютерной преступности, изучено состояние, структура динамики компьютерной преступности в современном Казахстане, криминогенных факторов, генерирующих их развитие.

Проблема уголовной политики в сфере информационной безопасности есть комплексная, системная социально-политическая и правовая проблема современного Казахстана, обусловленная общими и специальными экономическими, политическими, духовными, методологическими, юридическими, уголовно-правовыми, криминологическими и иными факторами. Она охватывает и смежные нормы уголовно-процессуального, уголовно-исполнительного и иных отраслей законодательства, обеспечивающих правовое регулирование такой разнородной сферы общественной жизни, как борьба с преступностью в сфере информатизации. Многочисленные исследования не привели пока к выработке достаточно точного и полного представления о феномене соответствующей государственной политики в сфере информатизации. При этом вопросы уголовной политики остаются неизученными. Последнее определяет новизну настоящего исследования. Предлагаемое исследование содержит научно обоснованные положения и выводы о теоретических основах профилактики преступлений в сфере информатизации и это определяет его научную значимость. Кроме того, обозначены основные проблемы по теме и обозначены основные направления их решения, что обуславливает его практическую значимость.

Методологическую основу исследования составляют научные положения уголовного права и криминологии о сущности преступления и преступности, их влиянии на состояние государственной и общественной безопасности. В ходе исследования современные концепции определения сущности преступления и преступности, выводы получены посредством качественного и количественного анализа социально-правовых, уголовно-правовых явлений и процессов.

Проведенный авторами правовой анализ позволяет представить рекомендации определению новых перспективных направлений уголовной политики Казахстана в сфере информационной безопасности и противодействия компьютерной преступности. Предполагаемые исследования могут внести реальный вклад в решение и преодоление международного аспекта имеющегося в сфере обеспечения информационной безопасности кризисного состояния. Преступления в сфере информационных технологий – особая сфера, поскольку сложившаяся система телекоммуникаций не имеет границ. Преступление может быть задумано в одной стране, пройти по коммуникациям трех-четырех других стран и совершиться в пятой. Эта обстоятельство предполагает необходимость налаживания взаимодействия с другими государствами.

Результаты, полученные в настоящей статье, можно использовать в учебном процессе, для написания учебников или учебных пособий и публикации статей по данной проблематике.

Ключевые слова: уголовная политика, информационная безопасность, компьютерная преступность, противодействие преступности.

Malikova Sh.B.[1], Omarova A.B.[2], Malikov D.B. [3]

[1]Candidate of Juridical Sciences, docent, e-mail: Sholpan.Malikova@kaznu.kz
[2]Candidate of Juridical Sciences, docent, e-mail: omar_17@mail.ru
[3]teacher, e-mail: Dauren.Malikov@kaznu.kz
al-Farabi Kazakh National University, Almaty, Kazakhstan

The Criminal Policy of the Republic of Kazakhstan in the Sphere of Informatization: Issues of Counteracting Computer Crime

The present article explores the problems of criminal policy in the field of information security, the development of criminal legislation in this area. The purpose of this article is to investigate the problems of criminal policy in the field of informatization or ensuring information security and the theoretical basis for countering computer crime. Within the framework of the research, the conceptual apparatus and theoretical foundations of the criminal policy in the field of information security and computer crime counteraction are clarified, the status and the structure of computer crime dynamics in modern Kazakhstan and criminal factors that generate their development are studied.

The problem of criminal policy in the sphere of information security is a complex, systemic socio-political and legal problem of modern Kazakhstan, conditioned by general and special economic, political, spiritual, methodological, legal, criminal, criminological and other factors. It also covers related norms of the criminal procedure, criminal executive and other branches of legislation that provide legal regulation of such a diverse sphere of public life as the fight against crime in the field of informatization. Numerous studies have not yet led to the development of a sufficiently accurate and complete picture of the phenomenon of the corresponding state policy in the field of informatization. At the same time questions of criminal policy remain unexplored. The latter determines the novelty of this study. The proposed study contains scientifically substantiated provisions and conclusions on the theoretical basis for the prevention of crimes in the field of informatization and this determines its scientific significance. In addition, the study identifies the main problems on the topic and outlines the main directions for their solution, which determines its practical importance.

The methodological basis of the research is the scientific provisions of criminal law and criminology on the nature of crime and criminality, their impact on the state and public security. In the course of the research, modern concepts of determining the nature of crime and criminality, the conclusions were obtained through a qualitative and quantitative analysis of socio-legal, criminal-legal phenomena and processes.

The legal analysis carried out by the authors makes it possible to provide recommendations for the definition of new promising avenues of the criminal policy of Kazakhstan in the field of information security and combating computer crime. Prospective studies can make a real contribution to solving and overcoming the international aspect of the crisis situation in the sphere of information security. Crimes in the field of information technology are a special sphere, since the existing telecommunications system have no borders. The crime can be conceived in one country, go through the communications of three or four other countries and be accomplished in the fifth. This circumstance presupposes the need to establish cooperation with other states.

The results obtained in this article can be used in the educational process, for writing textbooks or training manual and publishing articles on this topic.

Key words: criminal policy, information security, computer crime, counteraction to crime.

Маликова Ш.Б.[1], Омарова А.Б.[2], Маликов Д.Б.[3]

[1]з.ғ.к., доцент, e-mail: Sholpan.Malikova@kaznu.kz
[2]з.ғ.к., профессор, e-mail: omar_17@mail.ru
[3]оқытушы, e-mail: Dauren.Malikov@kaznu.kz
әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы қ.

Ақпараттандыру саласындағы Қазақстан Республикасының қылмыстық саясаты: компьютерлік қылмыстылыққа қарсы іс-қимыл мәселелері

Аталған мақалада ақпараттық қауіпсіздікті қамтамасыз ету аясындағы қылмыстық саясаттың, осы саладағы қылмыстық заңнаманы дамыту мәселелері зерттелген. Мақаланың мақсаты – ақпараттандыру немесе ақпараттық қауіпсіздікті қамтамасыз ету аясындағы және компьютерлік қылмыстылыққа қарсы тұрудың теориялық негіздерінің мәселелерін зерттеу. Зерттеу шеңберінде

ақпараттық қауіпсіздікті қамтамасыз ету аясындағы ұғымдық аппарат, осы саладағы қылмыстық саясаттың және компьютерлік қылмыстылыққа қарсы тұрудың теориялық негіздері нақтылаған, қазіргі Қазақстандағы компьютерлік қылмыстылықтың жай-күйі зерделеніп, динамикасы мен құрылымына, олардың дамуына әсер ететін криминогендік факторлар талданған.

Ақпараттық қауіпсіздік аясындағы қылмыстық саясат мәселесі жалпы және арнайы экономикалық, саяси, рухани, методологиялық, заңи, қылмыстық-құқықтық, криминологиялық және басқа да факторлармен шартталған заманауи Қазақстанның кешенді, жүйелі әлеуметтік-саяси және құқықтық мәселесі. Ол ақпараттандыру аясындағы қылмыстылықпен күрес сынды қоғамдық өмірдің әртүрлі саласын құқықтық реттеуді қамтамасыз ететін аралас қылмыстық-процестік, қылмыстық атқару заңнамасының және басқа да салаларының нормаларын қамтиды. Алуан түрлі зерттеулер ақпараттандыру аясындағы сәйкес мемлекеттік саясат феномені туралы нақты және жеткілікті көзқарасты қалыптастырған жоқ. Яғни, қылмыстық саясат сұрақтары әзірге жеткілікті дәрежеде зерттелмеген қалпында. Осы мән-жай аталған зерттеудің жаңалығын анықтайды. Ұсынылып отырған зерттеу ақпараттандыру аясындағы қылмыстардың алдын алудың теориялық негіздері туралы ғылыми негізделген ұсыныстар мен қорытындыларды беріп, оның ғылыми маңызын айқындайды. Сонымен қатар, тақырып бойынша негізгі мәселелер белгіленген және оларды шешудің негізгі бағыттары айқындалып, тақырыптың тәжірибелік құндылығын шарттаған.

Зерттеудің методологиялық негізін қылмыс және қылмыстылықтың мәні туралы, олардың мемлекеттік және қоғамдық қауіпсіздіктің жағдайына әсері туралы қылмыстық құқық және криминологияның ғылыми ережелері құрайды. Зерттеу барысында қылмыс және қылмыстылықтың мәнін анықтаудың заманауи тұжырымдамалары, қорытындылар әлеуметтік-құқықтық, қылмыстық құқықтық құбылыстар мен үдерістерді сапалық және сандық талдау жолымен алынған.

Авторлар арқылы жүргізілген құқықтық талдау ақпараттық қауіпсіздік және компьютерлік қылмыстылыққа қарсы тұру аясындағы Қазақстанның қылмыстық саясатының жаңа бағыттарын анықтауға қатысты ұсыныстар жасауға мүмкіндік береді. Аталған зерттеулер ақпараттық қауіпсіздікті қамтамасыз ету аясындағы халықаралық аспектіні шешу және жеңуге қатысты нақты үлес қосуы мүмкін. Ақпараттық технологиялар аясындағы қылмыстар – орын алып отырған телекоммуникациялар жүйесі шексіз болғандықтан ерекше ая болып табылады. Қылмыс бір елде ойластырылып, үш-төрт елдің коммуникацияларынан өтіп, бесінші елде жасалуы мүмкін. Аталған жағдай басқа мемлекеттермен өзара ынтымақтастықты қалыптастыру қажеттілігін білдіреді.

Мақалада алынған нәтижелерді оқу үдерісінде, оқулықтар мен оқу құралдарын және аталған мәселеге қатысты мақалалар жариялау барысында қолданыла алынады.

Түйін сөздер: қылмыстық саясат, ақпараттық қауіпсіздік, компьютерлік қылмыстылық, қылмыстылыққа қарсы тұру.

Сложившийся за последние годы эмпирический опыт противодействия преступности в сфере информатизации характеризуется превентивными средствами и нуждается в научном обобщении и интерпретации. Его научное осмысление приобретает особую актуальность с принятием нового Уголовного кодекса РК, поскольку в настоящее время практика предупреждения преступности в сфере информатизации складывается во многом стихийно, без единой руководящей идеи, нередко представляет собой импульсивные реакции на вызовы преступной среды и обострение криминальной ситуации. В этой связи возникает необходимость своевременного глубокого теоретического изучения новых правовых явлений в сфере уголовной политики, каковыми и являются компьютерная преступность и информационная безопасность.

Актуальность исследования обусловлена, в первую очередь, ростом компьютерных преступлений. За последние десять лет сети Интернет превратились в виртуальную площадку, в пространство, где люди имеют возможность выражать идеи, заниматься общественной деятельностью и пр. На сегодняшний день сети Интернет играют важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами как с использованием компьютера, так и банкомата, и других платежных систем, прокладываем маршруты, ищем хорошие рестораны, узнаем любую интересующую нас информацию. Конечно, понятно, что все эти действия зависят от информационных технологий. В связи с этим многие пользователи Интернета подвергаются атакам со стороны киберпреступников. По материалам сайта www.crime.vl.ru. котики, проституция и насильственная преступность, безусловно, останутся, но большинство преступников из иных сфер переориентируются в компьютерную.

На сегодняшний день отсутствует научно обоснованная целостная концепция уголовной политики в сфере обеспечения информационной безопасности, поскольку научные исследования практически не проводились. Многие вопросы требуют изучения, поэтому необходимо разработать научно обоснованный терминологический аппарат. До сих пор не раскрыто полностью, что относится к сфере информационных технологий в казахстанском законодательстве, хотя этим термином правоохранительные органы оперируют. К примеру, часто используется термин «преступления в сфере информационных технологий». Само понятие информации вызывает много споров и наиболее распространенными определениями являются те, которые содержатся в словарях [1]. При этом нет единого и достаточно точного представления о понятии, предмете и структуре этого феномена и в научной литературе. Многочисленные исследования понятия «уголовная политика» не привели пока к выработке достаточно точного и полного представления о феномене соответствующей государственной политики в сфере информатизации. Само понятие уголовной политики является предметом научных исследований и вызывает дискуссии [2-4]. Деятельность государства в сфере борьбы с преступностью (целиком либо в той или иной ее части) принято именовать уголовной политикой [3]. Однако, несмотря на многочисленные исследования, до сих пор отсутствует единство мнений в вопросе о содержании этого понятия, его значении и соотношении с иными родственными, так называемыми смежными понятиями. Требуют изучения и вопросы определения направлений установления социального контроля над соответствующими видами преступности в сфере информатизации с помощью правовых и организационно-тактических средств.

Объектом исследования выступили общественные отношения, складывающиеся между субъектами по вопросам противодействия компьютерной преступности и их отражение в уголовно-правовой теории и правоприменительной практике.

Предметом исследования стало состояние, структура и проблемы противодействия компьютерной преступности и вопросы совершенствования уголовного законодательства.

Целью исследования является изучение состояния, структуры, динамики компьютерной преступности в современном Казахстане, анализ криминогенных факторов, генерирующих развитие компьютерной преступности в современном Казахстане.

Методологическую основу исследования составили положения общенаучного диалектического метода познания социальных явлений. В процессе исследования использовались классические методы исследования, в том числе методы сравнительного, правового, системного и институционального анализов.

Область применения – деятельность законодательных органов по совершенствованию нормативных актов, деятельность правоохранительных органов по совершенствованию мер противодействия компьютерной преступности, учебный процесс, сфера юридической науки.

Высокая общественная опасность преступлений, совершаемых в сфере компьютерной информации, большое количество потерпевших, установленный и более значительный скрываемый материальный ущерб делают борьбу с этим негативным явление актуальной, как и то, что преступность в сфере компьютерной информации все шире используется в контексте организованной преступной деятельности и, особенно, деятельности террористических организаций, которые все активнее начинают использовать в своей противозаконной деятельности новейшие информационные технологии и компьютерную технику. Террористические акты в США 11 сентября 2001 года, которые сегодня называют «цифровым Перл-Харбором», и другие терракты, имевшие место в последние годы, ярчайшее тому подтверждение [5].

Вышеуказанные проблемы подверглись изучению в рамках проекта.

В первую очередь исследовано состояние компьютерной преступности в Республике Казахстан. При этом установлено, что Интернет, с одной стороны, позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой – породил новые, неизвестные еще совсем недавно мировому сообществу виды общественно опасных посягательств. По статистике, за последние десять лет отмечается постоянный рост количества пользователей Интернетом в Казахстане, в частности, отмечается, по данным TNS Web Index, что интернет – единственный растущий медиаканал в Казахстане, охват которого почти в 2 раза превышает охват прессы. В июле 2015 года количество интернет-пользователей в РК достигло 3,47 млн. То есть 71% населения страны в возрасте от 12 до 54 лет заходят в сеть минимум не реже одного раза в месяц. В 2016 году этот

показатель по прогнозам специалистов может достигнуть 4,5 млн. человек [3].

В ходе сбора и анализа литературы нами были использованы не только работы разных специалистов, статистические данные, опубликованные в интернет-источниках, но и научные труды известных отечественных и зарубежных ученых, в которых отмечается, что если ранее считалось, что компьютерная преступность – явление, присущее только развитым компьютеризированным зарубежным странам, и по причине слабой компьютеризации, т.е. недостаточного внедрения в производственные и общественные отношения информационных технологий, у нас отсутствует. Именно это обстоятельство и привело к отсутствию сколько-нибудь серьезных научных исследований вообще. Вместе с тем особенно теперь известная проблематика стала предметом широкого научного диспута и не только в кругах отечественной правовой науки [6; 7].

Определенное внимание уделено современному состоянию компьютерной преступности в нашей стране. В результате исследования сформулированы выводы, основной из которых сводится к тому, что по мнению большинства специалистов, в настоящее время мощный прогресс технологии привел к изменению структуры и качества компьютерных преступлений и, соответственно, картины компьютерной преступности. Это само по себе заслуживает интенсивного научного внимания, в том числе и со стороны криминологов. Преступность в сфере компьютерной информации, и особенно в Интернете, имеет тенденцию к значительному росту в части статей УК РК, предусматривающих неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных программ для ЭВМ. Отмечается, что состояние современной компьютерной преступности во многом определяется тенденцией переноса центра тяжести на совершение компьютерных преступлений с использованием компьютерных сетей и, прежде всего, Интернета, в котором в результате развивается нелегальный рынок [8].

Преступления в сфере компьютерной информации чаще всего стали совершаться организованно (группой компьютерных преступников), а также все шире используются в контексте организованной преступной деятельности и, прежде всего, в сфере экономической деятельности. С повышением уровня компьютеризации общества может усилиться киберактивность террористов. В связи с этим рекомендуется определять преступления в сфере компьютерной информации (компьютерные преступления) как предусмотренный уголовным законом противоправный, виновный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ, а также нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда, подлежащим уголовно-правовой охране [9].

Сегодня все осложняется еще, главным образом тем, что и изучение, и расследование данного вида преступления требует обязательных знаний в области информационных технологий. И в науке, и на практике ощущается острая нехватка юристов, обладающих глубокими знаниями в этой сфере. Это само по себе представляет собой серьезную проблему, над решением которой нужно работать системно, постоянно с учетом постоянного развития информационных технологий.

Кроме того, в настоящее время недостаточно изучены личность участника и причины преступлений в сфере компьютерной информации, а также меры противодействия такому виду преступности. В этой связи эти вопросы были изучены в рамках проекта. В итоге сделан вывод, что компьютерный преступник (хакер) – это, как правило, мужчина в возрасте от 18 до 24 лет (отмечается тенденция снижения возраста); с высоким уровнем образования, часто технического. Компьютерный преступник проявляет склонность к совершению компьютерных преступлений на продолжающейся основе, хотя статистически это сложно выявить, можно даже сказать, что не выявляется. Вместе с тем единой характеристики личности участника преступности в сфере компьютерной информации быть не может, что связано с их типологическим многообразием [10]. В связи с этим проведена типологизация компьютерных преступников по особенностям мотивации преступного поведения и степени устойчивости антиобщественной направленности, по уровню подготовленности и преступной специализации. Одной из характерных особенностей лиц, совершающих киберпреступления, является устойчивое стремление к паразитическому образу жизни, отсутствие какой-либо профессии, постоянного места работы, определенного места проживания. Составление обобщенного криминологического портрета личности компьютерного преступника в ходе

исследования проведено на основе материалов судебной и следственной практики, а также изучения зарубежного опыта обеспечения информационной безопасности [11; 12].

В ходе исследования структуры и динамики компьютерной преступности в Республике Казахстан выяснилось, что структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии компьютерных преступлений как преступлений специфических не существует.

Анализ криминогенных факторов, генерирующих развитие компьютерной преступности в современном Казахстане, показал, что значительное место в продуцировании компьютерной преступности также занимает виктимность обладателей компьютерной информации вследствие слабой организации охраны компьютерной информации и того, что ЭВМ характеризуется технической уязвимостью, в этой связи приоритет борьбы с компьютерной преступностью должен быть отдан мерам профилактического свойства. Под факторами в ходе исследования понимаются детерминанты, которые определяющим образом влияют на развитие известного рода преступности. Исследование показало, что факторы преступности в сфере компьютерной информации заложены в социально-экономической, социально-политической и социально-психологической сферах. В связи с уменьшающейся стоимостью и возрастающей миниатюризацией электронных компонентов сегодня возможным сделали самые современные технические средства стали доступными для широких слоев населения. Вместе с тем эта в целом положительная тенденция несет в себе и негативный потенциал, о чем свидетельствуют рост их статистической выявляемости, который по всем подсчетам будет усиливаться по мере увеличения концентрации вычислительных ресурсов, их территориальной распределенности, одновременного доступа к ресурсам многих пользователей [11]. Поэтому действенные меры борьбы с преступностью в сфере компьютерной информации, как представляется, состоят в преодолении ограниченности национального законодательства в русле формирования единой правовой базы, направленной против компьютерной преступности, а также в русле усиления гражданской, административной и уголовной ответственности. Основная рекомендация сводится к определению в качестве основного направления борьбы с преступностью в сфере компьютерной информации становление и развитие правового фундамента в сфере Интернета путем принятия Закона «О правовом регулировании использования сети Интернет». И поскольку абсолютной защиты компьютерной информации не существует, значительное место в предупреждении компьютерной информации должно принадлежать мерам технического и организационного характера. Важнейшее место в борьбе с преступлениями в сфере компьютерной информации должно отводиться политико-организационным, организационно-административным и организационно-администраторским мерам. Однако все меры предупреждения компьютерных преступлений будут эффективными только тогда, когда они будут использоваться все вместе, т.е. комплексно.

Литература

1 Сабитов Д. Информационная безопасность Казахстана: защита данных и смыслов. – Астана, 2015. – 68 с.

2 Назаров Р.И. Роль информации об этнической принадлежности в борьбе с дискриминацией: опыт государств. Этнологический мониторинг переписи населения / под ред. В.В. Степанова. – М.: ИЭА РАН, 2011. – 552 с.

3 Турлаев А.В., Шәкірова А.Б. Правовое обеспечение информационной безопасности в Республике Казахстан // Вестник КарГУ, 2013 // https://articlekz.com/article/6210

4 Ernst & Young. (n.d.). Global Information Security Survey. Retrieved 12 3, 2012, from

5 http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

6 Gary McGraw, S. M. (2012, September). BSIMM. Retrieved from http://bsimm.com/download/

7 Gerber, M., & Solms, R. v. (2008). Information security requirements – Interpreting the legalaspects. Computers & Security, 124-135.

8 Höne, K., & Eloff, J. (2002). Information security policy – what do international information security standards say. Computers & Security, 402-409.

9 Polkinghorne, D. E. (2005). Language and Meaning: Data Collection in Qualitative Research. Journal of Counseling Psychology, 52 (2), 37–145.

10 Susanto, H., Almunawar, M.N., & Tuan, Y.C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences, 23-29 .

11 Taleb, N.N. (2001). Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets. New York: Random House.

12 Verheul, E. (2011). Introduction to information security Lecture #1. Radboud University, Nijmegen. von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security. The information management journal, 371-376.

References

1 Danyar Cabitov. (2015). Informatsionaya bezopasnost Kazahstana: zachita dannyh I smyslov. – p.68.

2 Nazarov R.I. (2011). Rol informatsii ob ietnichescoi prinadlejnosti v borbe s descriminatsiei: opyt gosudarstv. Ietnologichescii monitoring perepisi naseleniya – M.: RAN – 552 p.

3 Turlaev A.B. Shakirova A.B. (2013). Pravovoe obespechenie informatsionnoi bezopasnosti v Respublike Kazahstan. Vestnik KarGU // https://articlekz.com/article/6210

4 Ernst & Young. (n.d.). Global Information Security Survey. Retrieved 12 3, 2012, from

5 http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

6 Gary McGraw, S. M. (2012, September). BSIMM. Retrieved from http://bsimm.com/download/

7 Gerber, M., & Solms, R. v. (2008). Information security requirements – Interpreting the legalaspects. Computers & Security, 124–135.

8 Höne, K., & Eloff, J. (2002). Information security policy – what do international information security standards say. Computers & Security , 402–409.

9 Polkinghorne, D. E. (2005). Language and Meaning: Data Collection in Qualitative Research. Journal of Counseling Psychology , 52 (2), 37–145.

10 Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences , 23–29 .

11 Taleb, N. N. (2001). Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets. New York: Random House.

12 Verheul, E. (2011). Introduction to information security Lecture #1. Radboud University, Nijmegen. von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security. The information management journal , 371–376.