Кириленко В. П., Алексеев Г. В.

Проблема обеспечения информационной безопасности государства в сфере распространения массовой информации

Кириленко Виктор Петрович

Северо-Западный институт управления — филиал РАНХиГС (Санкт-Петербург)
Заведующий кафедрой международного и гуманитарного права
Доктор юридических наук, профессор
Заслуженный юрист Российской Федерации
intlaw@szags.ru

Алексеев Георгий Валерьевич

Северо-Западный институт управления — филиал РАНХиГС (Санкт-Петербург)
Профессор кафедры международного и гуманитарного права
Кандидат юридических наук, доцент
intlaw@szags.ru

РЕФЕРАТ

Вопросы обеспечения информационной безопасности государства неразрывно связаны с политическими, экономическими и правовыми гарантиями реализации свободы слова и самовыражения в международном информационном пространстве. В современных политико-правовых условиях в равной степени опасны и недопустимы проявления цензуры и злоупотребления свободой массовой информации, самоизоляция и экстремизм, необъективность и безразличие в отношении тех событий, которые происходят в международной системе. В нарождающейся мультимедийной реальности угрозы безопасности связаны как с техническими особенностями передачи данных, так и с экономической природой общественных отношений в виртуальной среде. В процессе обеспечения информационной безопасности первостепенное значение приобретает устойчивое развитие информационной инфраструктуры гражданского общества и индустрии производства массовой информации.

КЛЮЧЕВЫЕ СЛОВА

информационная безопасность, средства массовой информации, медиабезопасность, информационные технологии, информационное право

Kirilenko V. P., Alekseev G. V.

The Problem of State Information Security in the Field of Mass Media

Kirilenko Viktor Petrovich

North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration (Saint-Petersburg, Russian Federation)
Head of the Chair of International and Humanitarian Law
Doctor of Science (Jurisprudence), Professor
Honored Lawyer of Russia
intlaw@szags.ru

Alekseev Georgy Valeryevich

North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration (Saint-Petersburg, Russian Federation)
Professor of the Chair of International and Humanitarian Law
PhD in jurisprudence, Associate Professor
intlaw@szags.ru

ABSTRACT

In the international media space the issues of ensuring information security of thestate is inseparably interrelated with the political, economic and legal guarantees for exercising freedom of speech and expression. Under modern political and legal conditions censorship and abuse of freedom of mass media, the isolation and extremism, bias and indifference to those events that occur in the

international system are equally dangerous and unacceptable. Emerging security threats of multimedia reality connected with the technical features of data transfer, and economic nature of social relations in a virtual environment. Mediaindustryandsustainable development of information infrastructure of civil society becomes prima priority for stateinformation security.

KEYWORDS
informationsecurity, massmedia, mediasecurity, information technologies, media law

Президент Российской Федерации В. В. Путин в рамках заседания Совета Безопасности, посвященного вопросам информационной безопасности, отметил, что «надежная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России в самом широком смысле этого слова». Он также обратил внимание на то, что «современную эпоху справедливо называют информационным веком. Новые технологии, глобальные коммуникационные сети охватывают практически все сферы деятельности человека и общества. Они на глазах меняют качество жизни людей, способствуют глобализации экономики и гуманитарного пространства»[1].

Во внутренней политике России с момента утверждения Доктрины информационной безопасности в 2000 г. под информационной безопасностью Российской Федерации понимается состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[2]. В процессе работы над проектом новой аналогичной Доктрины понятие информационной безопасности было расширено, оно стало охватывать состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства.

Вопросы обеспечения информационной безопасности государства неразрывно связаны с политическими, экономическими и правовыми гарантиями реализации свободы слова и самовыражения в международном информационном пространстве [2]. В современных политико-правовых условиях в равной степени опасны и недопустимы проявления цензуры и злоупотребления свободой массовой информации, самоизоляция и экстремизм, необъективность и безразличие в отношении тех событий, которые происходят в международной системе. Увеличение количества тех национальных интересов, для которых особое значение имеет защищенность информационной сферы жизни российского общества, в целом соответствует парадигме постиндустриальной социальной формации. Национальная информационная безопасность становится всеобъемлющим институтом государственной политики, что существенно усложняет административные процедуры по защите конкретных интересов в сфере производства и распространения информационных сообщений.

Поскольку реализуемая странами Запада «политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления» [4, с. 21], вопросы эффективного обеспечения информаци-

[1] Владимир Путин проводит заседание Совета Безопасности, посвященное вопросам противодействия угрозам национальной безопасности в информационной сфере. 1 октября 2014 [Электронный ресурс]. URL: http://www.putin-today.ru/archives/5920.

[2] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895) // Российская газета от 28 сентября 2000. № 187.

онной безопасности имеют важное значение для сохранения суверенитета и устойчивого развития страны.

Субъекты обеспечения информационной безопасности в зависимости от собственной компетенции выделяют тот или иной аспект системы национальной информационной безопасности, который представляет особую значимость непосредственно для них, задействует те сегменты информационной инфраструктуры, за безопасность в рамках которых ответственны конкретные государственные органы. Вместе с тем информационная безопасность обеспечивается в сфере компьютерных технологий, в средствах массовой информации и сетях связи общего пользования, в архивном и библиотечном деле, закрытых информационных системах. Информационный суверенитет государства предполагает не только «верховенство и независимость государственной власти при формировании и реализации информационной политики» [3, с. 21], но и предполагает «активное участие государственных органов и институтов гражданского общества в глобальной конкуренции на международном рынке массовой информации» [1, с. 373].

В результате активного проникновения компьютерных технологий в социально-культурные процессы современного общества фактически в рамках системы обеспечения информационной безопасности сформировались три относительно самостоятельных института: медиабезопасность, безопасность информационных технологий, защита информации от несанкционированного доступа и утечки. Эти основные составляющие института информационной безопасности нормативно объединяются в стратегическую концепцию защиты национальных интересов в информационной сфере. *Защита информации* — в значительной степени техническая проблема, которая решается техническими методами, *безопасность информационных технологий* определяется доступностью информационных систем и технологий в современном мире и зависит от уровня экономического развития и качества образования населения, в свою очередь *медиабезопасность,* как информационная безопасность в сфере массовой информации, является важнейшим компонентом эффективной государственной политики в медиасфере.

Чем выше уровень информатизации в социальных процессах, тем выше риски и шире спектр угроз информационной безопасности в части утечки информации и несанкционированного доступа к ней, в то же время возникает необходимость внедрять информационные технологии, улучшающие качество и производительность труда. Субъекты, участвующие в предоставлении услуг информационных сетей (абоненты, сервис-провайдеры, контент-провайдеры, провайдеры сети, поставщики «облачных» технологий, системы электронных или мобильных платежей), влияют на эффективность системы информационной безопасности. Каждый из этих участников имеет в распоряжении терминал сети и поэтому является потенциальной угрозой безопасности.

Расследование нарушений безопасности требует сбора данных из всего комплекса источников угроз. Кроме того, существование различных механизмов для доступа к сети (проводной, беспроводной, поддержка 3G и т. д.) создает множество точек доступа, которые могут использоваться для несанкционированного доступа и неправомерного использования. Обнаружение угроз безопасности требует постоянного обмена информацией между всеми субъектами обслуживания сетевых устройств [6]. При этом политики безопасности транснациональных корпораций, участвующих в предоставлении услуг социальных сетей, могут иметь существенные различия, что затрудняет взаимодействие между ними.

Допустимая степень активности защиты своих интересов в сфере компьютерной безопасности в последние годы стала одной из наиболее спорных тем, поднятой в рамках научной дискуссии по вопросу способов обеспечения информационной безопасности в современных социальных сетях. Отсутствие понимания принципи-

альных отличий вредоносных программ от средств активной защиты и блокировки вредоносного контента создает сложности в выработке универсального подхода к информационной безопасности [9].

Международная сеть интернет за последние 30 лет превратилась из академической информационной системы в глобальное средство массовой коммуникации, имеющее жизненно важное значение для мировой коммерции и политики, основанное на принципах открытости и совместного использования данных, которые имеют первостепенное значение для существования глобальной сети в ее современном качестве. Стратегическое представление о медиабезопасности, как об информационной безопасности в сфере массовых коммуникаций, формируется на основе алгоритмов решения тех практических задач, которые стоят перед государственными институтами в современных информационных сетях связи общего пользования. Угрозой безопасности страны в информационной сфере стало отставание политических и правовых институтов государства от темпов развития систем глобальной коммуникации, что обуславливает расширение спектра угроз информационной безопасности интересам частных лиц в различных сферах народного хозяйства страны.

Традиционные административные алгоритмы и регламенты, направленные на обеспечение национальной безопасности, работают в информационной сфере недостаточно эффективно. Интенсивность развития информационных систем и технологий требует гибкой и адаптивной системы медиакоммуникаций, ключевым свойством которой является способность к саморегулированию и самовосстановлению. Транспарентность государственных границ в системе международного общения, технологическая простота и легкость, с которой действия могут быть выполнены в рамках элементов глобальной сети связи, расположенных в районах, географически удаленных от абонента сети, не всегда позволяют соблюдать традиционные законы и формальности в современной системе массовых коммуникаций.

Краеугольным и не до конца решенным вопросом обеспечения информационной безопасности является правовая юрисдикция над общественными отношениями в социально-технических коммуникативных системах. Отсутствие универсального представления о юрисдикции в киберпространстве значительно усложняет понимание места и времени совершения актов медиакоммуникаций всеми участниками международного общения и субъектами политического процесса в частности.

Изначально многими сетевыми администраторами применялся принцип территориальной привязки интернет-коммуникаций к месту нахождения того терминала, через который осуществляется распространение информации. Такой физический подход используется для защиты границ государства и способствует внедрению соответствующих технологий для управления коммуникациями. Однако такой подход, проникая с уровня национальной безопасности в корпоративную культуру, становится все более деструктивной тенденцией по отношению к единству глобальной сети и отрицательно сказывается на популярности корпоративных ресурсов.

С момента начала работы интернета как сети связи общего пользования формирующаяся завеса безопасности, по справедливому замечанию американского специалиста в сфере информатики Вильяма (Билла) Чесвика, была «своего рода хрустящей оболочкой вокруг мягкого, тягучего центра» [7], которая до сих пор оказывает декоративное влияние на информационные сети связи. Система информационной безопасности широко использовала сеть брандмауэров — фильтров, способных как блокировать интернет-сайты с нежелательным контентом (черный список), так и в значительной мере блокировать все, кроме того, что необходимо для работы (белый список). Такие подходы к информационной безопасности, изначально внедренные в практику работы большинства организаций, способны обеспечить защиту информации, однако ограждая от взаимоувязанной глобальной

сети локальные ресурсы, системы безопасности создают угрозы другого порядка, затрудняют обработку информационных сообщений.

Скорость обработки информации, в условиях уплотняющейся конкуренции, становится одним из ключевых показателей защищенности информационной системы. В процессе развития глобальной сети все более широкое распространение и значение для нашей социальной и экономической жизни приобретают электронная торговля, новостные медиаресурсы и мультимедийная культура. Обеспечение целостности киберпространства зависит от комплекса технических, экономических, правовых мер, отражающих политику расширения возможностей человека посредством внедрения в жизнь информационных технологий.

Надлежащая практика защиты информации необязательно должна быть сложной и многоуровневой технической системой. Известный специалист в сфере компьютерной безопасности из Университета Родса (ЮАР) Барри Ирвин отмечает, что наиболее важная задача, стоящая перед всеми заинтересованными сторонами в рамках кибернетической безопасности, — повышение общей осведомленности об основных угрозах безопасности, решение которой способствует снижению вредоносной активности, исходящей из корпоративных информационных систем [9].

Основными участниками создания норм поведения в глобальной компьютерной сети являются частные корпорации, контролирующие предоставление телекоммуникационных услуг. При этом широкое распространение компьютерных технологий оказывает влияние на поведение пользователей систем технических устройств. Методы и инструменты защиты информации призваны обеспечить сохранность персональных данных и тайну частной жизни, однако соблазн узнать чужие тайны нередко оказывается сильнее любых мер безопасности [11, p. 4]. Медиакорпорации в силу их вовлеченности в процессы разработки программного обеспечения получают практически неограниченный доступ ко всему контенту глобальной сети, создают угрозы административного характера, связанные с рисками злоупотребления, полученными в силу технологического превосходства правами.

Технологические системы информационной безопасности получили весьма ограниченное распространение не только по причине своей ненадежности и высокой стоимости постоянной модернизации, но и в силу их неудобства для пользователей, сопряженного с постоянными рисками дополнительных расходов, в связи с утратой оперативного доступа к системам хранения и обработки информации. С одной стороны, мероприятия по защите информации должны использовать самые прогрессивные технологические разработки [13; 14], которые имеют существенную стоимость и отрицательно влияют на конкурентоспособность продукции предприятий; с другой стороны, технологическая сложность систем защиты информации отрицательно влияет на оперативность доступа к актуальной информации. Канадский профессор из Университета Онтарио Стефан Марш отмечает, что в большинстве сфер народного хозяйства обеспечить информационную безопасность, сохраняя при этом его социально-экономическую целесообразность, возможно лишь в той мере, в какой это соответствует уровню образования и культуры пользователей социальных сетей [12].

Информационная безопасность в таких условиях приобретает значение некой благоприятной парадигмы, к которой следует стремиться, однако обеспечить ее в полной мере чрезвычайно сложно в силу комплекса технических и социальных ограничений. В сложных технических системах неизбежны неполадки, со своей стороны человеческий фактор также определяет ряд угроз: пользователи могут иметь недостаток веры, понимания, терпения по отношению к мерам безопасности, которые существуют в компьютерных системах.

Многие зарубежные специалисты в сфере информатики полагают, что системы безопасности социальных сетей связи и других информационных ресурсов не ориентированы на потребности и способности пользователей, а подчинены логике некого образного духа безопасности, продиктованного техническими алгоритмами. В процессе реализации политики, направленной на усложнение систем безопасности в ходе своеобразной «гонки вооружений» в сфере кибернетической безопасности, существуют риски утраты доверия к техническому прогрессу как к фактору, благоприятно сказывающемуся на качестве жизни и доступности социальных благ для каждого человека без какой бы то ни было дискриминации.

Сложный этап в эволюции информационных систем связан с угрозой уменьшения интереса к материалам информационных сетей на фоне расширения спектра потенциальных угроз интересам абонентов. На наш взгляд, современные вызовы информационной безопасности связаны не только с увеличением числа кибератак, но и сопряжены с нарождающимися технологиями социальной инженерии, наслаивающимися на ставшие привычными вредоносные программы. Система социальных угроз в информационной сфере развивается значительно быстрее, чем формируются политико-правовые институты противодействия нарождающимся опасностям. Расширенные механизмы безопасности, лучшие пароли, более сложные процедуры входа в систему и ряд других технических решений в сфере безопасности не отвечают интересам рядовых пользователей компьютеров.

С тех пор как в 1974 г. американские ученые Ричард Барнет и Рональд Мюллер обратили внимание на то, что транснациональные корпорации конкурируют друг с другом в разработке все более изощренных средств защиты информации, ситуация не изменилась [5]. Разработанные и внедренные антивирусные технологии, с одной стороны, защищают информацию [14], а с другой — причиняют неудобства пользователю, которому эти системы безопасности фактически мешают работать на компьютере. В частности, профессор из Университета Виктории (Мельбурн, Австралия) Наташа Дуайер обоснованно полагает, что необходимо искать более человеко-ориентированный подход к безопасности, основанный на социальных нормах, способных обеспечить комфорт и доверие при работе с современными мультимедиа-системами.

Вместе с тем политика транснациональных корпораций идет вразрез с парадигмой доверия в отношениях с пользователями. Секретарь Совета Безопасности Российской Федерации Н. П. Патрушев на совещании во Владивостоке 26 августа 2015 г. отметил «наличие в информационных системах (органов государственной власти) программных средств иностранных технических разведок» и раскритиковал чиновников за использование иностранных сервисов Google, Yahoo, WhatsApp[1]. Вместе с тем очевидно, что конкурентоспособных отечественных разработок в сфере мультимедийных сервисов явно недостаточно.

По нашему мнению, уровень социальной медиабезопасности также зависит от удобства средств массовой коммуникации для ее целевой аудитории. В этом контексте основными угрозами информационной безопасности становятся все более низкое качество контента и навязывание медиакорпорациями собственных представлений о действительности. Если в технической составляющей информационной безопасности сложилось представление о «переднем плане доверия» [8] — способности технологического устройства представлять информацию пользователям на основе программных решений, ориентированных на доверие к конкретным ресурсам, то можно предположить, что именно федуциарность является одним из основных принципов обеспечения информационной безопасности в рамках всего

[1] Патрушев: в системах госвласти нашли иностранное разведывательное ПО [Электронный ресурс]. URL: http://www.vesti.ru/doc.html?id=2656749 (дата обращения: 20.09.2016).

спектра социальных институтов, испытывающих потребность в защищенности собственных интересов в информационной сфере.

Недоверие, которое возникает по отношению к материалам средств массовой информации низкого качества, распространяется в процессе потребления их продукции на всю медиаиндустрию и становится критической угрозой для безопасности страны. Реализуемая отдельными медиаструктурами в рамках социально-политических процессов концепция «свободного» выбора между неприятным и потенциально еще более неприятным раскручивает спираль недоверия к материалам средств массовой информации со стороны населения.

В нарождающейся мультимедийной реальности угрозы безопасности связаны как с техническими особенностями передачи данных, так и с экономической природой общественных отношений в виртуальной среде. В процессе обеспечения информационной безопасности первостепенное значение приобретает устойчивое развитие информационной инфраструктуры гражданского общества, неразрывно связанное с индустрией производства массовой информации. Интеграция социально-психологических понятий доверия и комфорта в вычислительные системы происходит на фоне сохранения устаревающих моделей работы с информацией в сфере документооборота, социального управления, производства массовой информации. В результате доверие к сетевым ресурсам растет, а понимание традиционной журналистики постепенно снижается.

Парадоксальность того, что интуитивный интерфейс мобильных устройств, призванный обеспечить понимание устройством команд пользователя, способствует доверию не только к надежности самого устройства, но и к содержанию тех сообщений, которое это устройство передает, имеет вполне очевидное социально-психологическое объяснение. Доверие пользователей к компьютерным системам определяется их функциональным назначением, комфорт зависит от степени понятности тех процессов обработки и передачи информации, в которых пользователь заинтересован. Использование антропоморфных принципов взаимодействия между пользователями и техническими системами формирует атмосферу безопасности, в которой доверие и комфорт — это принципы гибкого информационно-просветительского подхода к рискам, существующим в социальных сетях. В практику работы информационных систем активно внедряются «модели доверия, интеграции с различными мобильными устройствами, уют, комфортный дизайн с поддержкой пользовательских интерфейсов, направленных на расширение удобства для пользователя в разных контекстах» [12].

Виртуальные реальности интернета проникают в актуальную политику, значительно быстрее и больше, чем это принято ожидать. В традиционных средствах массовой информации имеется тенденция к имплементации мультимедийного формата распространения информации, однако это не добавляет комфорта и мало влияет на доверие аудитории к журналистам. Внедрение информационных технологий в производство средств массовой информации часто имеет противоположный результат и привносит недоверие и дискомфорт в работу предприятий медиаиндустрии и руководящих ими государственных органов, поскольку преследует иные цели, игнорируя обозначенную выше парадигму доверия в сфере информационной безопасности.

Атмосфера комфорта, доверия и компетентности в среде участников производства и распространения массовой информации является основным показателем информационной безопасности в социальных информационных сетях. Развитие современных средств массовой информации возможно исключительно в условиях их полезности и удобства для массовой аудитории, интересы которой определяют состояние социально-культурной сферы жизни общества. В данном контексте медиабезопасность зависит от понимания медиаиндустией и аудиторией интересов друг друга, их готовности к прогрессивным переменам.

Литература

1. *Кириленко В. П., Алексеев Г. В.* Международное право и информационная безопасность государств: монография. СПб. : СПб ГИКиТ, 2016.
2. *Кириленко В. П., Алексеев Г. В.* Особенности правового положения субъектов международной журналистики // Управленческое консультирование. 2014. № 6 (66). С. 24–32.
3. *Кучерявый М. М.* Информационное измерение политики национальной безопасности России в условиях современного глобального мира: дисс. д-ра полит. наук. СПбГУ, 2014.
4. *Шамахов В. А., Балашов А. И.* Новая геополитическая реальность и ее влияние на стратегию экономического и социального развития России // Управленческое консультирование. 2016. № 1 (85). С. 22–30.
5. *Barnet Richard J., Müller Ronald E.* Global Reach: The Power of the Multinational Corporations. New York, 1974.
6. *Bihina Bella M. A., Olivier M. S., Elo J. H. P.* A fraud management system architecture for next-generation networks // Forensic Science International. 2009. № 185. P. 51–58.
7. *Cheswick W. R.* The Design of a Secure Internet Gateway / Summer Usenix Conference. Anaheim, CA, June 1990. P. 233–237.
8. *Dwyer N.* Traces of Digital Trust: An Interactive Design Perspective. PhD thesis, School of Communication and three Arts, Faculty of Arts, Education and Human Development. Victoria University, 2011.
9. *Irwin Barry V. W.* Standing your ground: current and future challenges in cyber defense / Theories and Intricacies of Information Security Problems. Potsdam : Universitätsverlag, 2013. P. 100–108
10. *Kiountouzis E. A., Kokolakis S. A.* Information systems security: facing the information society of the 21st century. London : Chapman & Hall, Ltd., 2008.
11. *Marsh S., Basu A., Dwyer N*. Security enhancement with foreground trust, comfort, and ten commandments for real people / Theories and Intricacies of Information Security Problems. Potsdam : Universitätsverlag, 2013. P. 1–7.
12. *Marsh S., Briggs P.* Defining and investigating device comfort / Proceedings of IFIPTM 2010.
13. *Pipkin D.* Information security: Protecting the global enterprise. New York : Hewlett-Packard Company, 2000.
14. *Spagnoletti P., Resca A.* The duality of Information Security Management: fighting against predictable and unpredictable threats // Journal of Information System Security. 2008, 4 (3). P. 46–62.

References

1. Kirilenko V. P., Alekseev G. V. *International law and information security of the states* [Mezhdunarodnoe pravo i informatsionnaya bezopasnost' gosudarstv]: monograph. SPb. : St.Petersburg State University of Film and Television [SPb GIKiT], 2016. 396 p. (rus)
2. Kirilenko V. P., Alekseev G. V. *Features of a legal status of subjects of the international journalism* [Osobennosti pravovogo polozheniya sub"ektov mezhdunarodnoi zhurnalistiki] // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2014. N 6 (66). P. 24–32. (rus)
3. Kucheryavyy M. M. *Information measurement of policy of national security of Russia in the conditions of the modern global world* [Informatsionnoe izmerenie politiki natsional'noi bezopasnosti Rossii v usloviyakh sovremennogo global'nogo mira]: Doctoral Dissertation. St. Petersburg State University [SPbGU], 2014. 374 p. (rus)
4. Shamakhov V. A., Balashov A. I. *New geopolitical reality and its impact on the strategy for economic and social development of Russia* [Novaya geopoliticheskaya real'nost' i ee vliyanie na strategiyu ekonomicheskogo i sotsial'nogo razvitiya Rossii] // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2016. N 1 (85). P. 22–30. (rus)
5. Barnet Richard J., Müller Ronald E. *Global Reach: The Power of the Multinational Corporations.* New York, 1974.
6. Bihina Bella M. A., Olivier M. S., Elo J. H. P. *A fraud management system architecture for next-generation networks* // Forensic Science International. 2009. № 185. P. 51–58.
7. Cheswick W. R. *The Design of a Secure Internet Gateway* / Summer Usenix Conference. Anaheim, CA, June 1990. P. 233–237.
8. Dwyer N. *Traces of Digital Trust: An Interactive Design Perspective.* PhD thesis, School of Communication and three Arts, Faculty of Arts, Education and Human Development. Victoria University, 2011.

9. Irwin Barry V.W. *Standing your ground: current and future challenges in cyber defense* / Theories and Intricacies of Information Security Problems. Potsdam : Universitätsverlag, 2013. P. 100–108
10. Kiountouzis E.A, Kokolakis S.A. *Information systems security: facing the information society of the 21st century.* London : Chapman & Hall, Ltd., 2008.
11. Marsh S., Basu A., Dwyer N. *Security enhancement with foreground trust, comfort, and ten commandments for real people* / Theories and Intricacies of Information Security Problems. Potsdam : Universitätsverlag, 2013. P. 1–7.
12. Marsh S., Briggs P. *Defining and investigating device comfort* / Proceedings of IFIPTM 2010.
13. Pipkin D. *Information security: Protecting the global enterprise.* New York : Hewlett-Packard Company, 2000.
14. Spagnoletti P., Resca A. *The duality of Information Security Management: fighting against predictable and unpredictable threats* // Journal of Information System Security. 2008, 4 (3). P. 46–62.