УДК 159.9.01

С.Н. СОКОЛОВА, д–р филос. наук, доцент
Заслуженный деятель науки и образования
Российской академии естествознания,
Университет гражданской защиты МЧС
Республики Беларусь, г. Минск

Т.В. КАЛЕНЧУК
ассистент кафедры биотехнологий
Полесский государственный университет,
г. Пинск, Республика Беларусь

Статья поступила 6 октября 2018г.

ГИБРИДНЫЕ РИСКИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

В представленной статье авторы акцентируют внимание на характеристике гибридных рисков, а также угрозах гибридных войн и культуре безопасности в информационном обществе.

Ключевые слова: *гибридные риски, гибридные войны, культура безопасности, коммуникация, информационное общество, информационная война.*

Введение. Интенсивное развитие современных информационных технологий, а также телекоммуникационная, интернет, цифровая среда неизбежно провоцируют кумулятивный эффект гибридных войн (бесконтактных войн) и появление гибридных рисков, которые во многом определяют экзистенциальные вопросы, воздействуя на рефлексию личности, модели социальной реальности и сферу безопасности.

Активная борьба за природные ресурсы между современными государствами уже сегодня становиться глобальной проблемой, требующей комплексного решения, особенно, в период геополитических конфликтов, финансово–экономических кризисов, информационных и гибридных войн (бесконтактных войн). Открытое противоборство на межгосударственном уровне становиться в информационном обществе не только вариантом решения региональных проблем, но рискованным явлением, имеющим серьезные последствия в планетарном масштабе. И не случайно вопросы, связанные со сферой безопасности человека, общества, государства становятся первоочередными. И действительно, сегодня достаточно часто в решении международных проблем практикуются кибератаки, сетецентрические военные действия, информационные, гибридные войны (бесконтактные войны), т.е. осуществляются террористические акты с применением взрывных устройств, биологического и химического оружия. Вследствие этого, авторская акцентуация на вопросах, связанных с гибридными рисками, угрозами гибридных войн в информационном обществе сегодня не случайна.

Во–первых, современная ситуация, связанная с вооруженными конфликтами в разных странах, свидетельствует о том, что объективно в социуме возникают гибридные риски, которые характеризуют деструктивную динамику, негативные последствия стихийных бедствий, вооруженных конфликтов, бесконтактных войн, актуализирующих, в том числе, и «механизм нравственности», иллюстрирующих амплитуду аксиологического движения современной цивилизации. И ни для кого сегодня не секрет, что в информационном обществе решение международных конфликтов, как это ни парадоксально, «… идет не столько за столом переговоров, сколько в горячих точках» [1, с. 4]. Именно поэтому гибридные риски в информационном обществе становятся актуальной проблемой в связи с современными кризисами и вооруженными конфликтами.

Во–вторых, гибридные риски носят комплексный характер, включая в себя широкий спектр военно–стратегических, социально–политических, информационных аспектов, сочетая методы ведения традиционной войны.

Гибридные войны включают в себя множество рычагов воздействия на социальные институты любого государства (финансово–экономическое давление, подрывная деятельность спецслужб, трансформация ценностей). Напомним, что информационно–аналитическая, организационно–адаптивная, межкультурно–посредническая, межличностная коммуникация в информационном обществе представляет собой самый эффективный вид социальных взаимодействий, достаточно мобильных (относительно автономных). Кроме этого, как правило, практикуется дезинформация, а также привлечение вооруженных сил с применением высокоточного оружия и нерегулярных вооруженных формирований на территории противника. При ведении гибридной войны, как правило, используются латентные технологии, а также привлекаются специально подготовленные маргиналы, военизированные формирования (группировки террористов), которые могут использоваться в сочетании со специальными подразделениями. Также, при осуществлении сетецентрических военных действий, современных кибератак источником организованного вторжения выступает не военная разведка (аналитические подразделения), а другие силы, преследующие реализацию таких целей, как финансово–экономическое давление, идеологическое воздействие для получения морально–психологических преимуществ, инициированное дипломатами, общественными организациями, гуманитарным воздействием (на международном уровне) и участием десантно–штурмовых сил, морской пехоты, спецназа. В тоже время, информационная экспансия, деструктивно направленная коммуникация привели к масштабным изменениям в приемах ведения гибридных войн (бесконтактных войн) с помощью обновленных форм, методов и средств, а также информационно–сетевых технологий, что особенно актуализирует вопросы, связанные с гибридными рисками в информационном обществе [2].

В–третьих, интерес к гибридным рискам, а также угрозам гибридных войн в информационном обществе не случаен, так как в эпоху развития техногенной цивилизации, информационно–телекоммуникационной инфраструктуры происходит переформатирование геополитического, финансово–экономического, военно–стратегического, социокультурного пространства и «… двухполюсная картина холодной войны уступает место намного более сложным отношениям в многополюсном, полицивилизационном мире» [3, с. 393].

Гибридные риски, как и угрозы гибридных войн, отражают сущность процессов, происходящих в полицивилизационном мире, что также характеризуется участием человека, общественных структур, государства в наращивании коммуникационной архитектуры, активизации цифровой среды, представляющей сегодня «цифровую опасность» (в рамках взаимной интеграции различных социумов). При этом, многоуровневая система веерных, многосложных, разновекторных социокультурных взаимодействий в информационном обществе, является результатом постоянно обновляющегося образовательного пространства.

Гибридные риски, как правило, включают в себя осуществление комплекса гибридных угроз различного типа: традиционные, нестандартные, масштабный терроризм,

подрывные действия, в ходе которых используются различные, нередко и инновационные технологии для более эффективного противостояния превосходящей военной силе (несанкционированные действия в информационной, финансовой, энергетической, демографической сфере, кибератаки, киберпреступления). Гибридные риски в информационном обществе возрастают при условии существования угроз гибридных войн: в случае активной информационной экспансии с целью переформатирования личности, группы, социума, которые находятся в эпицентре конфликта (информационно–телекоммуникационные технологии, интернет, цифровая среда, образовательное пространство); при целенаправленном воздействии информационно–телекоммуникационной инфраструктуры на человека и общество, находящееся на периферии конфликта. В данном контексте, именно социокультурное взаимодействие в информационном обществе рассматривается авторами статьи, как некая результирующая позиция и «… наиболее динамичная в аспекте микроструктуры (на уровне малых социальных групп) и относительно устойчивая в аспекте макроструктуры (уровень больших социальных групп) …» [4, с. 31].

Основная часть. Сфера безопасности информационного общества в настоящее время находится в процессе своего становления и формирование ее системы пока не завершено. Практически параллельно с социальными преобразованиями весьма энергично в начале третьего тысячелетия стали решаться вопросы обеспечения безопасности национальных интересов. Это зафиксировано многими учеными и специалистами, которые полагают, что фактически сфера безопасности стала расширяться и приобретать совершенно иное качественное состояние. Это обновленное состояние и детерминирует дальнейшие научные разработки, теории и концепции.

Напомним, что специфика сферы безопасности проявляется в том, что она носит в большей степени общественно–государственный характер и зачастую распространяется на информационное общество. Кроме того, безопасность во многих своих проявлениях носит политический характер, зависит от сформировавшейся системы агрегирования, артикуляции национальных интересов, а также идеологии государства. Но в некоторой степени сфера безопасности одновременно и субъективна, поскольку максимально зависит от действий различных субъектов. Именно поэтому безопасность понимается как неотъемлемая часть общественного бытия, в котором формируются условия для наиболее эффективной реализации защиты интересов человека, общества и государства.

В таком качестве безопасное существование связано на практике с основными сферами общественной жизни и многочисленными запросами, потребностями различных субъектов, а также ответными действиями по оптимизации защиты как этих интересов, так и процессов их реализации. Безопасность в максимальной степени постоянно проявляется в других сферах: экономической, политической, социальной и духовной (культура безопасности). При этом многоуровневая система веерных, многосложных и разновекторных взаимодействий в информационном обществе, является итогом постоянно обновляющегося образовательного пространства, что является темой для отдельной научной статьи.

Важно учитывать тот факт, что гибридные риски включают в себя реализацию комплекса гибридных угроз различного типа: традиционные, нестандартные, масштабный терроризм и подрывные действия, в ходе которых используются различные, нередко инновационные технологии для противостояния превосходящей военной силе (кибератаки, действия в информационной, финансовой, энергетической, демографической сфере, киберпреступления).

В связи с этим, существующие альтернативы развития и процессы взаимодействия современных стран свидетельствуют о том, что:

1) активизация диалогичность взаимоотношений между государствами (военно–стратегическое, экономическое, политико–правовое, социокультурное сотрудничество) позволяет, в итоге, уменьшить градус недоверия в решении важных вопросов международной безопасности;

2) ускорение разработку новых стратегических систем и видов вооружений, которые являются катализатором изменений системы взаимоотношений между

государствами в многомерной социальной реальности;

3) оптимизация поиск путей взаимодействия в области укрепления системы международной безопасности, наращиванием информационно–политической составляющей в деятельности альянса в рамках современной мировой эклектики, а также активного процесса гибридизации (кардинальное перерождение НАТО из «реликта холодной войны» в обновленную организацию, обеспечивающую перманентный процесс разновекторного доминирования на мировой арене).

В этом случае, разработка стратегических приемов противодействия угрозам гибридных войн должна включать следующие элементы:

– четкое определение источников угроз гибридных войн (спецоперации) и оперативная оценка гибридных рисков и угроз (управление рисками, управление защитой от чрезвычайных ситуаций, антикризисное управление);

– организация максимально эффективного предупреждения «гибридного вторжения» в процессе реализации деятельности регулирующих центров, имеющих наднациональный характер (учебные Центры по подготовке военных специалистов, Центр кибероперацій, Центр передового опыта по проблемам гибридных угроз в информационном обществе);

– более активная военно–стратегическая адаптация в многополюсном мире и целенаправленная профессионализация сферы безопасности (создание новых центров силы) и неизбежной гибритизации альянса (с целью глобального доминирования). Стратегический баланс сил, как показывает практика, зависит от участия партнеров (союзников) в реализации полномасштабных переговоров по реформированию учреждений сферы безопасности информационного общества;

– минимизировать вмешательство во внутренние дела независимых стран и локализовать распространение западных ценностей без учета национальных интересов различных государств (цветные революции, этноконфессиональные конфликты).

Сложность современной геополитической ситуации заключается в том, что разноплановое, многоуровневое финансово–экономическое давление на различные государства наносит непоправимый ущерб интересам Республики Беларусь, а значит, становиться менее эффективной национальная безопасность, что может привести к нестабильности в обществе и, в конечном итоге, и к глобальному вооруженному конфликту или третьей мировой войне.

Угрозы гибридных войн требуют особых усилий государственных институтов с целью активизации международного сотрудничества в сфере безопасности. В современном социуме базовым элементом гибридной войны являются действия латентных сил, которые возникают непосредственно по инициативе и финансовой поддержке представителей различных государств. Динамика международных отношений такова, что перманентные военные конфликты, кризисы свидетельствуют о том, что сегодня важно перейти к комплексной безопасности, минимизируещей информационный терроризм, сетецентрические военные действия, киберпреступность.

Гибридная война, как правило, предполагает дезинформирование граждан, и в этом случае становится возможным при решении внешнеполитических и внутриполитических проблем использование вооруженных сил, применение высокоточного, химического оружия, нерегулярных вооруженных формирований на территории противника. Системно осуществляется подбор, синтез и анализ необходимой информации, где источником организованного вторжения выступает не военная разведка и не аналитические подразделения различных ведомств. Это специфическая коммуникативно–разновекторную экспансию, которая деструктивно воздействует на социальную реальность, изменяя информационные ресурсы и переформатируя общественные отношения. От других вооруженных конфликтов гибридная война отличается тем, что она базируется не на применении силы, а на всестороннем использовании информации.

Гибридная война представляет собой специфическое, очень сложное явление, аккумулирующее в себе все виды современной войны, и, как правило, носят универсальный характер, актуализируя, тем самым, геополитические факторы экономической дестабилизации.

Современная интеграция, информатизация, а также борьба различных государств за перераспределение мировых ресурсов акцентирует внимание исследователей на гибридных рисках, а также необходимости выработки более эффективных методов системного противодействия угрозам гибридных войн. И совершенно не случайно, что «… все страны мира сейчас решают одну масштабную задачу – необходимость обеспечивать устойчиво–безопасное развитие и актуальные потребности граждан, одновременно максимально инвестируя в новые технологии» [5, с. 141].

Развитие современных коммуникационных технологий (особенно Интернета, социальных сетей) свидетельствует о необходимости использования политической элитой, экспертами, научным сообществом, военными специалистами информационной составляющей и семантического поля, постоянно изменяющегося под воздействием специально инициированных вирусов, современных универсальных компьютерных программ. И нельзя забывать, что в информационном обществе доминирует информационный терроризм, а значит, угрозы гибридных войн становятся реальностью и, в этом случае, важно акцентировать внимание на информационной безопасности, так как в результате гибридного вторжения, например, сохраняемая банками информация, может не выполнить свое предназначение, а значит, потерять в результате кибератаки свою конфиденциальность.

Исходя из этого, авторы статьи предлагают конкретные методы системного противодействия угрозам гибридных войн:

1) метод агрегирования, антимонопольного развития инфраструктуры информатизации, как синтеза программной реализации социально–экономического развития (интеграционная внешнеэкономическая деятельность в области информатизации, учитывающая общенациональную стратегию, в том числе, и стратегию рисков);

2) метод приоритетности в развитии интенсивного финансирования научно–технических разработок, особенно в сфере безопасности (робототехника, искусственный интеллект, андроидное строительство, нанобиотехнологии, космическая промышленность, наноиндустрия);

3) метод согласованности в решении вопросов, связанных с информатизацией, а также создание более эффективных территориальных инфраструктур с целью реализации системного подхода в создании единого информационного пространства;

4) метод координирующего воздействия и реализации социально–экономического ориентированного развития, обеспечивающего преемственность, стабильность, единство в результате государственной политики информатизации;

5) метод прогнозирования перспектив развития информационно–семантического поля на основе современных коммуникационных технологий (информационно–аналитическое обеспечение и мониторинг национальной безопасности).

В контексте такой авторской интерпретации, необходимо обратить особое внимание на такие интегральные показатели (маркеры), как, во–первых, информационно–семантическое поле, информационные инфраструктуры социума, современная индустрия переработки информации при условии обязательного соблюдения прав и свобод граждан.

Во–вторых, приоритетность в обеспечении информатизации социальной реальности (материального производства), более профессионального регионального управления для реализации эффективной информационной государственной политики, подготовки специалистов в области информационных технологий (более эффективная защита информационных ресурсов, теле–видео–телекоммуникационных систем).

И, в–третьих, накопление, сохранность информационных ресурсов, особенно, в сфере безопасности для интенсификации информационной индустрии с целью выхода на международные рынки.

К сожалению, сегодня во многих современных социумах доминирует аномальное окно возможностей, что деструктивно влияет на общественные отношения, смещая акценты в пользу дестабилизирующих факторов, что происходит по причине того, постоянно инициируя маргинальный элемент, усиливающий негативные тенденции, повышающий криминогенность социальной реальности. Для более эффективного

противодействия угрозам гибридных войн сегодня важно перейти к комплексной безопасности и более адекватно реагировать на возникающие гибридные риски, особенно в цифровой среде, например, специально инициированные компьютерные вирусы, вредоносные программы и кибератаки.

Общегосударственная стратегия в эпоху глобальной интеграции предполагает более активное использование комплексного подхода в сфере безопасности, а также активизацию многоуровневой и более эффективной информационно–аналитической деятельности в сфере безопасности. Следовательно, комплексная безопасность становиться приоритетной в информационном обществе, по причине того, что гибридные риски и существующие угрозы гибридных войн постепенно приобретают универсальный характер.

Заключение. Создание высокотехнологичного производства в эпоху бурного развития компьютерно–сетевых программ, внедрения в повседневную жизнь человека нанобиотехнологий, искусственного интеллекта, а также интенсивное применение разноплановых научных изобретений, несомненно, детерминируя сферу безопасности информационного общества.

Актуализируя вопросы, связанные с гибридными рисками в информационном обществе надо обязательно учитывать, что «… пересмотр приоритетов и акцентов в интерпретации проблемы безопасности и перенос их интересов государства на интересы самого человека, становится актуальной разработка проблем информационной безопасности личности и, в частности, информационной безопасности …» [6, с. 64].

Гибридные риски и гибридная война, как относительно новые научные категории, носят универсальный характер и характеризуют различные уровни экзистенции современной личности, общества, государства, что, в свою очередь, предполагает обеспечения комплексной безопасности.

В процессе глобализирующегося мира, динамично осуществляется переход большого потока информации в цифровую форму и актуализация вопросов, связанных с угрозами гибридных войн и ценностями безопасности. И надо учитывать, что развитие информационного общества связано не только с процессами глобализации, интеграции, но и с угрозами гибридных войн (бесконтактных войн) и «механизмом нравственности». Именно поэтому сегодня важно акцентировать внимание на ценностях безопасности, так как, в этом случае, позитивная (созидающая) социальная адаптация личности позволит субъектам осознанно стремиться к интеллектуальной экономике, инклюзивному рынку, гуманистическим культурным стандартам, более эффективному социокультурному сотрудничеству в планетарном масштабе. Современная конверсия социальных институтов, частичное разрушение системных связей, цементирующих белорусское государство, как никогда ранее, актуализируют проблему гибридных рисков, угроз гибридных войн (бесконтактных войн), так как средства информационного обеспечения «… образуются совокупностью информационных фондов банков данных, используемых в процессе решения задач обеспечения информационной безопасности, а также средств их актуализации» [7, с. 53].

Список литературы

1. Лукашенко, А.Г. Наша общая цель – построение сильного и безопасного государства / А.Г. Лукашенко // Белорусская думка, 2017. – № 5. Май.– С. 30–20.
2. См.: Соколова, С.Н. Риски и угрозы гибридных войн в современном обществе: парадоксы реальности / С.Н. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2017. – № 1. – С. 35–41; Соколова, С.Н. Аксиологический смысл безопасной экзистенции человека: сигма безопасности / С.Н. Соколова, А.А. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2017. – № 1. – С. 24–29; Соколова, С.Н. Онтология безопасности и гуманистическая модернизация современного общества / С.Н. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – 2017. – № 1. – С. 35–48; Соколова, С.Н. Угрозы гибридных войн: обеспечение безопасности человека и общества / С.Н. Соколова, А.А. Соколова // Предупреждение и ликвидация чрезвычайных ситуаций:

противодействие современным вызовам и угрозам. Сборник научных трудов. – Минск : УГЗ, 2017. – С. 36–38; Соколова, С.Н. Информационное общество: образовательное пространство и национальная безопасность / С.Н. Соколова, Т.В. Каленчук // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – 2018. – № 1. – С. 36–43.

3. Хантингтон, С. Столкновение цивилизаций / С. Хантингтон ; пер. с англ. Т. Велимеева. – М.: АСТ: АСТ МОСКВА, 2006. – 603 с.
4. Степин, В.С. Человек. Деятельность. Культура / В.С. Степин. – СПб : СПбГУП, 2018. – 800 с.
5. Фомин, М.В. Технологии качества жизни и постиндустриальная эпоха / М.В. Фомин // Вопросы философии. – 2016. – № 3. – С. 141.
6. Панарин, И.Н. Технология информационной войны / И.Н. Панарин. – М., 2003.
7. Сулакшин, С.С. Категория «безопасность»: от категориального смысла до государственного управления / С.С. Сулакшин / Национальная безопасность: научное и государственное управленческое содержание : материалы Всеросс. науч. конф., 4 дек. 2009 г., Москва / Центр пробл. анал. и гос.–упр. проект. М.: Научный эксперт, 2010. – 736 с.

Резюме. В статье авторы рассматривают гибридные риски как научную дефиницию, включающую многообразный спектр общественных отношений: финансово–экономических, социально–правовых, информационно–аналитических, организационно–адаптивных, межкультурно–посреднических, межличностных коммуникации, во многом определяющих направленность процессов, в которых безопасность понимается как неотъемлемая часть безопасной экзистенции человека, общества и государства.

В случае начала (ведения) гибридной войны используются латентные технологии, привлекаются специально подготовленные маргиналы, военизированные формирования, которые могут использоваться в сочетании со специальными подразделениями, что особенно актуализирует гибридные риски в информационном обществе.

Интерес к гибридным рискам и угрозам гибридных войн, а также к культуре безопасности в информационном обществе не случаен, так как в эпоху развития информационно–телекоммуникационной инфраструктуры в полицивилизационном мире, как правило, происходит активизация ангажированной цифровой среды и возникает «цифровая опасность». При этом многоуровневая система веерных, многосложных и разновекторных взаимодействий в информационном обществе является итогом постоянно обновляющегося коммуникационного пространства.

В этом контексте необходимо учитывать тот факт, что гибридные риски, как правило, включают в себя реализацию комплекса гибридных угроз различного типа: традиционные, нестандартные, масштабный терроризм и подрывные действия, в ходе которых используются различные, нередко инновационные технологии для противостояния превосходящей военной силе.

В таком качестве безопасное существование связано на практике с основными сферами общественной жизни и многочисленными запросами, потребностями различных субъектов, а также ответными действиями по оптимизации защиты как этих интересов, так и процессов их реализации.

Таким образом, создание высокотехнологичного производства в эпоху бурного развития компьютерно–сетевых программ, внедрения в повседневную жизнь человека нанобиотехнологий, искусственного интеллекта, а также интенсивное применение разноплановых научных изобретений, несомненно, детерминирует сферу безопасности информационного общества. В этом контексте необходимо учитывать тот факт, что гибридные риски включают в себя реализацию комплекса гибридных угроз различного типа: традиционные, нестандартные, масштабный терроризм и подрывные действия, в ходе которых используются различные, нередко инновационные технологии для противостояния превосходящей военной силе (кибератаки, действия в информационной, финансовой, энергетической, демографической сфере, киберпреступления). Современная интеграция стран, борьба различных государств за перераспределение мировых

ресурсов особенно актуализирует гибридные риски в информационном обществе.

Abstract. In the article the authors consider hybrid risks as a scientific definition, including a diverse range of social relations: financial, economic, social, legal, information–analytical, organizational–adaptive, intercultural–intermediary, interpersonal communication, largely determining the direction of the processes in which security is understood as an integral part of the safe existence of man, society and the state. In this regard, the specificity of the security sphere is manifested in the fact that it is more of a public–state nature and often extends to the information society. In addition, security in many of its manifestations is political in nature, depends on the formed system of aggregation, articulation of national interests, as well as the ideology of the state. But to some extent, the security sphere is both subjective, because it depends as much as possible on the actions of various actors. That is why security is understood as an integral part of social life, which forms the conditions for the most effective implementation of the protection of human interests, society and the state.

In the case of the beginning (conduct) of a hybrid war, latent technologies are used, specially trained marginalized, paramilitary groups are involved, which can be used in combination with special units, which especially actualizes hybrid risks in the information society.

Interest in hybrid risks and threats of hybrid wars, as well as in the culture of security in the information society is not accidental, as in the era of information and telecommunications infrastructure development in the police world, as a rule, there is an activation of the biased digital environment and there is a "digital danger". At the same time, the multi–level system of fan, multi–complex and multi–vector interactions in the information society is the result of constantly updated communication space.

In this context, it is necessary to take into account the fact that hybrid risks, as a rule, include the implementation of a complex of hybrid threats of various types: traditional, non–standard, large–scale terrorism and subversive actions, in which various, often innovative technologies are used to confront the superior military force.

As such, a safe existence is associated in practice with the main spheres of public life and numerous requests, the needs of various actors, as well as response actions to optimize the protection of both these interests and the processes of their implementation.

Thus, the creation of high–tech production in the era of rapid development of computer–network programs, the introduction of nanobiotechnology, artificial intelligence, as well as the intensive use of diverse scientific inventions, undoubtedly determining the security of the information society. In this context, it is necessary to take into account the fact that hybrid risks include the implementation of a complex of hybrid threats of various types: traditional, non–standard, large–scale terrorism and subversive actions, in which various, often innovative technologies are used to confront the superior military force (cyberattacks, actions in the information, financial, energy, demographic sphere, cybercrime). Modern integration of countries, the struggle of various States for the redistribution of world resources especially actualizes hybrid risks in the information society.

SOKOIOVA Svetlana N., Doctor of Philos. Sc., Associate Professor
University of Civil Defence of Ministry of Emergencies of the Belarus
Minsk, Republic of Belarus

KALENCHUK Tatyana V.
Assistant Department of Biotechnology
Polessky State University, Pinsk, Republic of Belarus

HYBRID RISKS IN THE INFORMATION SOCIETY

In the present article, the authors focus on the essential characteristics of hybrid risks, as well as the threats of hybrid wars and the culture of security in the information society.

Keywords: *hybrid risks, hybrid wars, culture security, communication, information society, information war.*

References

1. Lukashenko A.G. Nasha obshhaja cel' – postroenie sil'nogo i bezopasnogo gosudarstva [Our common goal – building a strong and safe state]. *Belaruskaja dumka* [Belarusian Dumka]. 2017, no 5, May, pp. 30–20. (In Russian)
2. Sokolova S.N. Riski i ugrozy gibridnyh vojn v sovremennom obshhestve: paradoksy real'nosti [Risks and threats of a hybrid war in modern society: the paradoxes of reality]. *Vestnik Polesskogo gosudarstvennogo universiteta. Serija obshhestvennyh i gumanitarnyh nauk* [Bulletin of the Polesie state University]. A series of social Sciences and Humanities. 2017, no 1, pp. 35–41(In Russian); Sokolova S.N., Sokolova A.A. Aksiologicheskij smysl bezopasnoj jekzistencii cheloveka: sigma bezopasnosti [Axiological meaning of the safe human being: Sigma security]. *Vestnik Polesskogo gosudarstvennogo universiteta. Serija obshhestvennyh i gumanitarnyh nauk* [Bulletin of Polessky state University. A series of social Sciences and Humanities]. 2017, no 1, pp. 24–29 (In Russian); Sokolova S.N. Ontologija bezopasnosti i gumanisticheskaja modernizacija sovremennogo obshhestva [Ontology of security and humanistic modernization of modern society]. *Vestnik Polesskogo gosudarstvennogo universiteta. Serija obshhestvennyh i gumanitarnyh nauk* [Bulletin of Polesie state University. A series of social Sciences and Humanities]. 2017, no 1, pp. 35–48(In Russian); Sokolova S.N., Sokolova A.A. Ugrozy gibridnyh vojn: obespechenie bezopasnosti cheloveka i obshhestva [The Threat of hybrid war: human security and society]. *Preduprezhdenie i likvidacija chrezvychajnyh situacij: protivodejstvie sovremennym vyzovam i ugrozam* [The Prevention and elimination of emergency situations: countering new challenges and threats]. Minsk: UGZ, 2017, pp. 36–38(In Russian); Sokolova S.N., Kalenchuk T.V. Informacionnoe obshhestvo: obrazovatel'noe prostranstvo i nacional'naja bezopasnost' [Information society: educational space and national security]. *Vestnik Polesskogo gosudarstvennogo universiteta. Serija obshhestvennyh i gumanitarnyh nauk* [Bulletin of the Polesie state University. A series of social Sciences and Humanities]. 2018, no 1, pp. 36–43. (In Russian)
3. Huntington S. *Stolknovenie civilizacij* [Clash of civilizations]. Per. with English. So Belieeve. Moscow, AST, 2006, 603 p. (In Russian)
4. Stepin V.S. *Chelovek. Dejatel'nost'. Kul'tura* [Man. Activity. Culture]. SPb : Spbgup, 2018, 800 p.
5. Fomin M.V. Tehnologii kachestva zhizni i postindustrial'naja jepoha [Technology of quality of life and post–industrial era]. *Voprosy filosofii* [Questions of philosophy]. 2016, no 3, pp.141. (In Russian)
6. Panarin I.N. *Tehnologija informacionnoj vojny* [Technology information war]. Moscow, 2003. (In Russian)
7. Sulakshin S.S. Kategorija «bezopasnost'»: ot kategorial'nogo smysla do gosudarstvennogo upravlenija [Category «security»: from the categorical meaning to public administration]. *Nacional'naja bezopasnost': nauchnoe i gosudarstvennoe upravlencheskoe soderzhanie* [National security: scientific and public management content]. 2009, Moscow. Scientific expert, 2010, 736 p. (In Russian)

Received 6 October 2018