Ограничение распространения кибероружия как фактор обеспечения безопасности в информационном мире

**Человек:** Предметом исследования являются проблемы кибербезопасности. Объектом исследования являются аспекты применения кибероружия, влияющие на международную и национальную кибербезопасность. В обзорной статье уточняются возможные подходы к ограничению применения подобного оружия.С развитием информационных технологий, межгосударственное противоборство приобретает новые формы, в том числе связанные с борьбой в киберпространстве. С учётом этого фактора, автором проведён обзор вопросов безопасности в киберпространстве и, в связи с ними, уточнение вопросов безопасности государства. Для анализа проблемы использовались сравнительный и системный методы, а также категорийный подход. Для формирования выводов применялся метод синтеза. Автор утверждает, что проблема несанкционированного применения кибероружия является комплексной и не может быть решена ни одним из государств мира самостоятельно, без вступления в кооперацию с другими участниками процесса. Для решения проблемы предлагается использовать подходы, аналогичные применяемым в настоящее время в области ограничения распространения вооружений и критичных технологий.

**Key words:** информационное противоборство, кибератаки, информационные провокации, кибероборона, предупреждение провокаций, кибероружие, нераспространение, международное регулирование, обязательства по нераспространению, безопасность цифрового общества

=================================

**FastText\_KMeans\_Clean:** Контроль распространения (поставок). "+" - однозначно присутствует, реализуется практически всегда;. "±" - может быть в ряде случаев. 2.Анализ существующих проблем и их возможных последствий. 3.Анализ подходов к противодействию. - персонификация разрабатываемых программ для идентификации их в случае применения, по аналогии с маркировкой обычного вооружения;. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия. Данные меры не простые и не самые быстрые по времени, но применить их насущно необходимо, пока очередная пропущенная кибератака не обернулась технологической или гуманитарной катастрофой глобального масштаба.

**Key words part:** 0.4814814814814815

=================================

**FastText\_KMeans\_Raw/:** Для ядерного оружия. Контроль за производством. Основаны эти опасения и на том, что с 2010 года в руководящих документах НАТО термин "киберзащита" (cyberbuck-defence), был заменён на понятие "кибероборона" (cyberbuck-defensive), что формально позволяет органам государственного управления относить кибератаки к угрозам, попадающим под действие статьи 5 Вашингтонского договора (Североатлантический договор, Вашингтон, Федеральный округ Колумбия, 4 апреля 1949 года об обеспечении коллективной безопасности). Например, как показывает анализ таблицы 1, путём выстраивания системы, аналогичной той, которая используется при формировании международных ограничений доступа к потенциально опасным технологиям [25,26,27]. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия.

**Key words part:** 0.5555555555555556

=================================

**FastText\_PageRank\_Clean/:** Для ядерного оружия. Контроль за производством. Контроль распространения (поставок). Контроль процесса повседневной эксплуатации. "+" - однозначно присутствует, реализуется практически всегда;. "–" - однозначно отсутствует;. Последнее вызывает особые опасения. 3.Анализ подходов к противодействию.

**Key words part:** 0.3703703703703704

=================================

**FastText\_PageRank\_Raw/:** Для ядерного оружия. Контроль за производством. Контроль распространения (поставок). Контроль процесса повседневной эксплуатации. "+" - однозначно присутствует, реализуется практически всегда;. "–" - однозначно отсутствует;. Последнее вызывает особые опасения. 3.Анализ подходов к противодействию.

**Key words part:** 0.3703703703703704

=================================

**Mixed\_ML\_TR/:** Что подтверждает актуальность организации противодействия составляющим процесса "непрямого" противоборства, в первую очередь – борьбе в киберпространстве. Таблица 1 – Отличительные особенности процесса контроля за распространением кибероружия (по состоянию на текущее время). Анализ содержания таблицы 1 показывает, насколько до настоящего времени не решена проблема контроля распространения кибероружия по сравнению с другими опасными вооружениями и технологиями. Атака аналогичного по типу вируса "Petya" в июне 2017 года временно вывела из строя телефонные сети и сайты промышленных предприятий в ряде стран: на Украине, в России, Италии, Дании, Германии. В то же время, как показывает практика кибератак и операций, проводимых в последние годы, существующие средства и методы обороны отдельных объектов или систем от атак из киберпространства, реализующие "реактивный" принцип управления, малоэффективны. Они обеспечивает вступление в противоборство уже после начала действий нападающих и проявления результатов атаки. Например, как показывает анализ таблицы 1, путём выстраивания системы, аналогичной той, которая используется при формировании международных ограничений доступа к потенциально опасным технологиям [25,26,27]. - разработка механизмов международного контроля за производством и распространением кибероружия и.т.п. В качестве технологических мер можно сформулировать:. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия.

**Key words part:** 0.5185185185185185

=================================

**MultiLingual\_KMeans/:** Что подтверждает актуальность организации противодействия составляющим процесса "непрямого" противоборства, в первую очередь – борьбе в киберпространстве. Таблица 1 – Отличительные особенности процесса контроля за распространением кибероружия (по состоянию на текущее время). Атака аналогичного по типу вируса "Petya" в июне 2017 года временно вывела из строя телефонные сети и сайты промышленных предприятий в ряде стран: на Украине, в России, Италии, Дании, Германии. В то же время, как показывает практика кибератак и операций, проводимых в последние годы, существующие средства и методы обороны отдельных объектов или систем от атак из киберпространства, реализующие "реактивный" принцип управления, малоэффективны. Они обеспечивает вступление в противоборство уже после начала действий нападающих и проявления результатов атаки. Например, как показывает анализ таблицы 1, путём выстраивания системы, аналогичной той, которая используется при формировании международных ограничений доступа к потенциально опасным технологиям [25,26,27].

**Key words part:** 0.5185185185185185

=================================

**Multilingual\_PageRank/:** Контроль за производством. Контроль распространения (поставок). "+" - однозначно присутствует, реализуется практически всегда;. "–" - однозначно отсутствует;. "±" - может быть в ряде случаев. Один из последних примеров – атака вируса "WannaСry", прекратившего в начале 2017 года на время функционирование десятков британских больниц, испанской корпорации Telefonica, крупнейшего железнодорожного перевозчика Германии Deutcshe Bahn, испанской сотовой компании "Телефоника". Атака аналогичного по типу вируса "Petya" в июне 2017 года временно вывела из строя телефонные сети и сайты промышленных предприятий в ряде стран: на Украине, в России, Италии, Дании, Германии. Этот тезис отражается в большинстве руководящих документов альянса [18,19].

**Key words part:** 0.3703703703703704

=================================

**RuBERT\_KMeans\_Without\_ST/:** Пример, подтверждающий последний тезис – экономические ограничения и санкции, используемые в своё время против СССР (впоследствии РФ), Ирана, КНДР и т.п. Законы развития общества неумолимы – спрос всегда рождает предложение: с углублением информатизации всех сфер общества появилась новая сфера межгосударственного противоборства: киберпространство. Возможность определить место применения, производителя, кем применено. В то же время, как показывает практика кибератак и операций, проводимых в последние годы, существующие средства и методы обороны отдельных объектов или систем от атак из киберпространства, реализующие "реактивный" принцип управления, малоэффективны. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия.

**Key words part:** 0.5555555555555556

=================================

**RuBERT\_KMeans\_With\_ST/:** Пример, подтверждающий последний тезис – экономические ограничения и санкции, используемые в своё время против СССР (впоследствии РФ), Ирана, КНДР и т.п. Законы развития общества неумолимы – спрос всегда рождает предложение: с углублением информатизации всех сфер общества появилась новая сфера межгосударственного противоборства: киберпространство. "+" - однозначно присутствует, реализуется практически всегда;. В то же время, как показывает практика кибератак и операций, проводимых в последние годы, существующие средства и методы обороны отдельных объектов или систем от атак из киберпространства, реализующие "реактивный" принцип управления, малоэффективны. Например, как показывает анализ таблицы 1, путём выстраивания системы, аналогичной той, которая используется при формировании международных ограничений доступа к потенциально опасным технологиям [25,26,27].

**Key words part:** 0.5185185185185185

=================================

**RUBERT\_page\_rank\_Without\_ST/:** Указанные факторы, наряду с несомненно положительным влиянием на развитие общества, порождают уязвимость систем, зависящих от коммуникационных связей. Контроль за производством. "–" - однозначно отсутствует;. 2.Анализ существующих проблем и их возможных последствий. Последнее вызывает особые опасения.

**Key words part:** 0.4074074074074074

=================================

**RUBERT\_page\_rank\_With\_ST/:** "–" - однозначно отсутствует;. "±" - может быть в ряде случаев. Последнее вызывает особые опасения. Во-первых , необходимо урегулировать международное и региональное законодательство в части предоставления хостинговых услуг. Наиболее вероятные из организационных мер в масштабе государства:.

**Key words part:** 0.4074074074074074

=================================

**RUSBERT\_KMeans\_Without\_ST/:** В то же время, сформулированные ранее особенности разработки и применения кибероружия порождают парадокс: оружие, потенциально обладающее не меньшей разрушительной мощью, чем ядерное, распространяется практически бесконтрольно. В то же время, проблема до настоящего времени не выведена на международный уровень, несмотря на предпринимавшиеся попытки [22,23,24]. Наиболее вероятные из организационных мер в масштабе государства:. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия.

**Key words part:** 0.4444444444444444

=================================

**RUSBERT\_KMeans\_With\_ST/:** Вышеуказанные отличия определяют ряд особенностей, характерных для развития кибероружия. Сложившаяся ситуация позволяет сделать вывод, что масштабы последствия кибератак будут возрастать с ростом уровня информатизации жизни и производства и, рано или поздно, могут обернуться глобальной катастрофой [13,14,15]. Применяемое в настоящее время законодательство практически не регулирует вопросы безопасности и распределения ответственности за нарушения в данной области. - организация ограничений на распространение кибероружия, вероятно, на тех же принципах, которые реализованы с ядерными вооружениями и ракетными технологиями.

**Key words part:** 0.4814814814814815

=================================

**RUSBERT\_page\_rank\_Without\_ST/:** 2)Широкие возможности обеспечения скрытности источника применения. Контроль процесса повседневной эксплуатации. "+" - однозначно присутствует, реализуется практически всегда;. "–" - однозначно отсутствует;. "±" - может быть в ряде случаев.

**Key words part:** 0.3703703703703704

=================================

**RUSBERT\_page\_rank\_With\_ST/:** 2)Широкие возможности обеспечения скрытности источника применения. Контроль за производством. "+" - однозначно присутствует, реализуется практически всегда;. "–" - однозначно отсутствует;. "±" - может быть в ряде случаев.

**Key words part:** 0.3703703703703704

=================================

**Simple\_PageRank/:** Их наличие обеспечивает возможность осуществления непрямого межгосударственного противоборства [1,2], в том числе через реализацию угроз уязвимостям информационно-коммуникационных сетей и, в итоге, существенно расширяют перечень проблем обеспечения безопасности государства [3,4,5,6]. Пример, подтверждающий последний тезис – экономические ограничения и санкции, используемые в своё время против СССР (впоследствии РФ), Ирана, КНДР и т.п. Законы развития общества неумолимы – спрос всегда рождает предложение: с углублением информатизации всех сфер общества появилась новая сфера межгосударственного противоборства: киберпространство. 1) В отличие от "традиционных" видов вооружения, с самого начала их разработки поставленных под государственный, а часто и межгосударственный контроль, кибероружие может производится "кустарно" и свободно распространяться. Анализ содержания таблицы 1 показывает, насколько до настоящего времени не решена проблема контроля распространения кибероружия по сравнению с другими опасными вооружениями и технологиями. Сложившуюся ситуацию необходимо критично осознать и на этой основе решить вопрос о введении правил разработки и распространения кибероружия, то есть перейти к "активным" принципам обороны. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия.

**Key words part:** 0.5555555555555556

=================================

**TextRank/:** Анализ содержания таблицы 1 показывает, насколько до настоящего времени не решена проблема контроля распространения кибероружия по сравнению с другими опасными вооружениями и технологиями. В то же время, сформулированные ранее особенности разработки и применения кибероружия порождают парадокс: оружие, потенциально обладающее не меньшей разрушительной мощью, чем ядерное, распространяется практически бесконтрольно. Исходя из этого, проблема противодействию кибероружию является глобальной, и ни одно государство не способно решить её в одиночку, применением частных защитных мер, таких, как внедрение международного стандарта ISO/IEC 27032:2012 "Information technology - Security techniques - Guidelines for cybersecurity", разрабатываемых на его основе государственных стандартов менеджмента безопасности серии ГОСТ Р ИСО/МЭК 2700Х, управления рисками ГОСТ Р ИСО/МЭК 27005-2010, оценки безопасности ГОСТ Р ИСО/МЭК 15408-2012, оценки рисков ГОСТ Р ИСО/МЭК ТО 18044-2007, проектирования систем безопасности ГОСТ Р ИСО/МЭК 21827-200 и других национальных нормативных документов, например, концепций информационной безопасности [20,21]. Во-вторых , учитывая, что процесс создания новых видов вооружения предотвратить невозможно, необходимо принять ряд организационных и технологических мер по ограничению распространения кибероружия. - разработка механизмов международного контроля за производством и распространением кибероружия и.т.п. В качестве технологических мер можно сформулировать:. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия.

**Key words part:** 0.5555555555555556

=================================

**TF-IDF\_KMeans/:** Влияние развития информационных технологий на безопасность усугубляется тенденцией расширения форм межгосударственного противоборства, переходом основных усилий в невоенную сферу, в том числе экономическую [7]. Кибероружие обладает рядом особенностей, отличающих его от "традиционных" видов вооружения. Анализ содержания таблицы 1 показывает, насколько до настоящего времени не решена проблема контроля распространения кибероружия по сравнению с другими опасными вооружениями и технологиями. В то же время, для других видов вооружения решения существуют, что позволяет надеяться на наличие возможностей разрешения аналогичных проблем и в части кибероружия. 2.Анализ существующих проблем и их возможных последствий. В то же время, как показывает практика кибератак и операций, проводимых в последние годы, существующие средства и методы обороны отдельных объектов или систем от атак из киберпространства, реализующие "реактивный" принцип управления, малоэффективны. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия. Данные меры не простые и не самые быстрые по времени, но применить их насущно необходимо, пока очередная пропущенная кибератака не обернулась технологической или гуманитарной катастрофой глобального масштаба.

**Key words part:** 0.6296296296296297

=================================

**Текст:** Нормальное функционирование современного общества определяется целым рядом факторов, связанных с развитием информационных технологий: увеличение количества и возможностей коммуникационных связей, рост номенклатуры и количества потребителей информации, например, появление интернета вещей (Internet of Things, IoT), в том числе промышленного (Industrial Internet of Things, IIoT) и, как итог, формирование «электронной» (цифровой, сетевой) экономики. Ещё раньше плоды информационной революции были реализованы в военной сфере: информатизация поля боя привела к появлению сетецентрических военных действий, обеспечивающих получение превосходства над противником за счёт повышения ситуационной осведомлённости и управляемости своих войск (сил). Указанные факторы, наряду с несомненно положительным влиянием на развитие общества, порождают уязвимость систем, зависящих от коммуникационных связей. Их наличие обеспечивает возможность осуществления непрямого межгосударственного противоборства [1,2], в том числе через реализацию угроз уязвимостям информационно-коммуникационных сетей и, в итоге, существенно расширяют перечень проблем обеспечения безопасности государства [3,4,5,6]. Что подтверждает актуальность организации противодействия составляющим процесса «непрямого» противоборства, в первую очередь – борьбе в киберпространстве.. . 1.Обзор особенностей применения кибероружия. Влияние развития информационных технологий на безопасность усугубляется тенденцией расширения форм межгосударственного противоборства, переходом основных усилий в невоенную сферу, в том числе экономическую [7]. Пример, подтверждающий последний тезис – экономические ограничения и санкции, используемые в своё время против СССР (впоследствии РФ), Ирана, КНДР и т.п.. Законы развития общества неумолимы – спрос всегда рождает предложение: с углублением информатизации всех сфер общества появилась новая сфера межгосударственного противоборства: киберпространство. Соответственно, появилось и новое средство борьбы в этом пространстве – кибероружие [8,9]. К кибероружию в настоящее время принято относить программное обеспечение или оборудование, предназначенные для нанесения ущерба в кибепрстранстве [10]. В более широком понимании, это специальные программные и программно-аппаратные средства, обеспечивающие целевое воздействие на информацию, как разрушающее, так и не разрушающее (модификацию). В условиях глобальной информатизации потенциальными объектами воздействия кибероружия являются элементы критической информационно-управляющей инфраструктуры всех областей атакуемого государства (сообщества) [11].. Кибероружие обладает рядом особенностей, отличающих его от «традиционных» видов вооружения.. 1)Специфическая область применения – киберпространство, в которой нет физических преград и государственных границ, практически неограниченная дальность распространения воздействия.. 2)Широкие возможности обеспечения скрытности источника применения.. 3)Нематериальность, облегчающая производство и распространение (копирование) средств воздействия.. Вышеуказанные отличия определяют ряд особенностей, характерных для развития кибероружия.. 1) В отличие от «традиционных» видов вооружения, с самого начала их разработки поставленных под государственный, а часто и межгосударственный контроль, кибероружие может производится «кустарно» и свободно распространяться.. 2) Кроме того, если для серийного производства обычного оружия необходимо достаточно мощное производство, однажды разработанные программные варианты кибероружия распространяются простым копированием. Для его производства не нужны крупные производственные мощности и специальное оборудование.. 3) Сложность противодействия до начала использования в связи с отсутствием признаков подготовки к применению. Проблемы определения, какого типа средствами и кем конкретно осуществлялось кибернападение.. Анализ все этих особенностей позволяет оценить признаки, отличающие кибероружие от «классического» с точки зрения контроля его распространения (таблица 1).. . Таблица 1 – Отличительные особенности процесса контроля за распространением кибероружия (по состоянию на текущее время). Признак. Для ядерного оружия. Обычное оружие. Кибероружие. Контроль за производством. +. ±. -. Контроль распространения (поставок). +. ±. -. Контроль процесса повседневной эксплуатации. +. -. -. Возможность определить место применения, производителя, кем применено. +. +. ±. В таблице:. «+» - однозначно присутствует, реализуется практически всегда;. «–» - однозначно отсутствует;. «±» - может быть в ряде случаев.. Анализ содержания таблицы 1 показывает, насколько до настоящего времени не решена проблема контроля распространения кибероружия по сравнению с другими опасными вооружениями и технологиями. В то же время, для других видов вооружения решения существуют, что позволяет надеяться на наличие возможностей разрешения аналогичных проблем и в части кибероружия.. . 2.Анализ существующих проблем и их возможных последствий. При этом, как показывает практика, применение кибероружия, как правило, приводит к очень существенным последствиям. Примерами могут служить атаки на объекты критической инфраструктуры венесуэльской нефтяной компании PDVSA, когда в результате атаки добыча нефти сократилась с 3 миллионов до 370 тысяч баррелей в сутки, атака вируса «Stuxnet» с целью срыва ядерной программы Ирана и многие другие [3]. Один из последних примеров – атака вируса «WannaСry», прекратившего в начале 2017 года на время функционирование десятков британских больниц, испанской корпорации Telefonica, крупнейшего железнодорожного перевозчика Германии Deutcshe Bahn, испанской сотовой компании «Телефоника». Проблемы возникли у российского «Мегафона», а также у информационных подразделений Министерства внутренних дел [12]. Атака аналогичного по типу вируса «Petya» в июне 2017 года временно вывела из строя телефонные сети и сайты промышленных предприятий в ряде стран: на Украине, в России, Италии, Дании, Германии. Анализ указанных и множества других инцидентов показывает, что последствия кибератак приобретают всё более глобальный характер: от локальных экономических проблем и технологических сбоев переходя к техногенным авариям с возможностью разрастания в глобальные экологические и техногенные катастрофы. Сложившаяся ситуация позволяет сделать вывод, что масштабы последствия кибератак будут возрастать с ростом уровня информатизации жизни и производства и, рано или поздно, могут обернуться глобальной катастрофой [13,14,15].. В то же время, сформулированные ранее особенности разработки и применения кибероружия порождают парадокс: оружие, потенциально обладающее не меньшей разрушительной мощью, чем ядерное, распространяется практически бесконтрольно. В том числе – в частные руки или к членам террористических организаций: компоненты кибероружия и услуги хакерских сообществ можно приобрести в Интернете [3,16,17]. Не миновал этот процесс и оружие промышленной разработки. На слуху ситуация, когда в 2016 году группа хакеров Shadow Brokers похитила ряд вредоносных программ, разработанных АНБ США и, в дальнейшем, применила их в собственных целях.. Таким образом, опасность несанкционированного распространения кибероружия постоянно растёт. В то же время, как показывает анализ тенденций, пока масштаб атак и их последствия непрерывно возрастают, их «авторов» не удаётся не только наказать, но даже идентифицировать.. Последнее вызывает особые опасения. Основаны эти опасения и на том, что с 2010 года в руководящих документах НАТО термин «киберзащита» (cyberbuck-defence), был заменён на понятие «кибероборона» (cyberbuck-defensive), что формально позволяет органам государственного управления относить кибератаки к угрозам, попадающим под действие статьи 5 Вашингтонского договора (Североатлантический договор, Вашингтон, Федеральный округ Колумбия, 4 апреля 1949 года об обеспечении коллективной безопасности). И, соответственно, отвечать на атаки, проведённые неизвестно кем и неизвестно откуда, реальными действиями против подозреваемого в них вероятного противника. И, при этом, в качестве одного из основных источников киберугроз США и страны НАТО считают, в том числе, нашу страну. Этот тезис отражается в большинстве руководящих документов альянса [18,19].. . 3.Анализ подходов к противодействию. В то же время, как показывает практика кибератак и операций, проводимых в последние годы, существующие средства и методы обороны отдельных объектов или систем от атак из киберпространства, реализующие «реактивный» принцип управления, малоэффективны. Они обеспечивает вступление в противоборство уже после начала действий нападающих и проявления результатов атаки. Иногда – очень разрушительных и требующих существенных затрат на восстановления повреждённой информационной и технологической инфраструктуры.. Исходя из этого, проблема противодействию кибероружию является глобальной, и ни одно государство не способно решить её в одиночку, применением частных защитных мер, таких, как внедрение международного стандарта ISO/IEC 27032:2012 «Information technology - Security techniques - Guidelines for cybersecurity», разрабатываемых на его основе государственных стандартов менеджмента безопасности серии ГОСТ Р ИСО/МЭК 2700Х, управления рисками ГОСТ Р ИСО/МЭК 27005-2010, оценки безопасности ГОСТ Р ИСО/МЭК 15408-2012, оценки рисков ГОСТ Р ИСО/МЭК ТО 18044-2007, проектирования систем безопасности ГОСТ Р ИСО/МЭК 21827-200 и других национальных нормативных документов, например, концепций информационной безопасности [20,21]. В то же время, проблема до настоящего времени не выведена на международный уровень, несмотря на предпринимавшиеся попытки [22,23,24]. То есть решение эффективного противодействия киберугрозам не найдено даже в самом общем виде.. Сложившуюся ситуацию необходимо критично осознать и на этой основе решить вопрос о введении правил разработки и распространения кибероружия, то есть перейти к «активным» принципам обороны. Например, как показывает анализ таблицы 1, путём выстраивания системы, аналогичной той, которая используется при формировании международных ограничений доступа к потенциально опасным технологиям [25,26,27].. Для реализации подобных мер и переходу к активным мерам противодействия потенциальным киберугрозам, потребуется выполнить ряд мероприятий.. Во-первых , необходимо урегулировать международное и региональное законодательство в части предоставления хостинговых услуг. Применяемое в настоящее время законодательство практически не регулирует вопросы безопасности и распределения ответственности за нарушения в данной области.. Во-вторых , учитывая, что процесс создания новых видов вооружения предотвратить невозможно, необходимо принять ряд организационных и технологических мер по ограничению распространения кибероружия.. Наиболее вероятные из организационных мер в масштабе государства:. - организация ограничений на распространение кибероружия, вероятно, на тех же принципах, которые реализованы с ядерными вооружениями и ракетными технологиями.. - разработка механизмов международного контроля за производством и распространением кибероружия и.т.п.. В качестве технологических мер можно сформулировать:. - персонификация разрабатываемых программ для идентификации их в случае применения, по аналогии с маркировкой обычного вооружения;. - реализация в разрабатываемом оружии обязательного требования идентификации пользователя в соответствии с правами доступа для предотвращения несанкционированного допуска к нему, даже в случае утери контроля и т.п.. Соответственно, с точки зрения ограничений в отношении частных лиц и организаций, представляется целесообразным введение ответственности на уровне международного законодательства не только за применение, но и за несанкционированное производство и распространение кибероружия.. . Заключение. Реализовать указанные меры не просто, но вполне реально, через создание системы международных договорённостей и согласованной корректировки внутреннего законодательства. Данные меры не простые и не самые быстрые по времени, но применить их насущно необходимо, пока очередная пропущенная кибератака не обернулась технологической или гуманитарной катастрофой глобального масштаба.