

ВООРУЖЕНИЯ БЕЗ КОНТРОЛЯ: СОВРЕМЕННЫЕ УГРОЗЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: 10.20542/2307-1494-2018-2-64-83

Аннотация В статье рассмотрены наиболее актуальные угрозы в информационной сфере, которые имеют глобальный и стратегический характер и представляют опасность для международного мира. Логика выбора угроз для анализа основана на классификации, представленной в официальных документах РФ. В соответствии с ней, выделяется применение информационно-коммуникационных технологий в целях: (а) военно-политического характера для осуществления враждебных действий и актов агрессии; (б) вредоносного воздействия на объекты критически важной государственной инфраструктуры; (в) интернет-пропаганды экстремизма и терроризма и интернет-рекрутинга. Выявлены признаки таких угроз и общемировые тенденции, способствующие росту рисков в этой сфере. Проанализированы военные средства, которые задействуются в проведении информационных операций. Рассмотрены примеры целенаправленного вредоносного воздействия на физические объекты критически важной инфраструктуры, а также истоки угроз, связанных с использованием интернета для преступной и террористической деятельности и осуществления информационно-психологического воздействия; сделаны практические рекомендации по минимизации рисков от вредоносного применения интернета. Сделан вывод о необходимости незамедлительного создания механизмов международного управления и контроля. Одним из них могут стать правила поведения государств в информационном пространстве, принятия которых под эгидой ООН целенаправленно добивается Россия. В заключении подчеркивается важная роль, которую должно играть экспертное сообщества и научно-образовательные учреждения на каждом этапе процесса принятия решений по профилактике и предотвращению угроз международной информационной безопасности и даны соответствующие рекомендации для научно-экспертного сообщества в этой сфере.

Ключевые слова международная информационная безопасность (МИБ), информационно-коммуникационные технологии (ИКТ), информационное пространство, кибервойна, кибероружие, информационная угроза, киберугроза, кибератака, ядерная программа Ирана, вредоносная компьютерная программа, "Stuxnet", "Duqu", "Wiper", "Flame", "Gauss", "MiniFlame", интернет-рекрутинг, интернет-пропаганда, кибертерроризм, экстремизм, информационно-психологическое воздействие, социальная сеть

Title Uncontrolled weapons: modern threats to international informational security

Abstract The article focuses on the most acute threats to international information security that have global and strategic nature and endanger international peace. Categorization of these threats is based on Russian official classification. It identifies threats that (a) involve misuse of information communication technologies (ICT) for military and political purposes, including hostile actions and acts of aggression; (b) harm to critical national infrastructure; (c) online propaganda and recruiting by extremists and terrorists. The article analyzes

Ромашкина Наталья Петровна – руководитель Группы проблем информационной безопасности ИМЭМО РАН, кандидат политических наук.

symptoms of such threats and global trends that contribute to growing risks of this type. Military means employed in information operations are also explored. The article reviews several cases of purposeful malicious actions against physical objects of critical infrastructure; reveals sources of threats of the use of the Internet for criminal and terrorist activity and information and psychological brainwashing; and offers practical recommendations on how to minimize risks caused by malicious use of the Internet. It also calls for the urgent creation of international governance and control mechanisms in this field. One of them could be a code of state conduct in the information space that is actively promoted by Russia at the UN. The article concludes by stressing the important role that the expert community and academic institutions should play at every step of the decision-making process on dealing with international information security threats and provides recommendations for academic and expert communities.

Keywords International Information Security (IIS), Information and Communication Technology (ICT), information space, cyber warfare, cyber weapon, informational threat, cyber threat, cyber-attack, Iran's nuclear program, malicious software, "Stuxnet", "Duqu", "Wiper", "Flame", "Gauss", "MiniFlame", online recruiting of adepts, Internet propaganda, cyber-terrorism, extremism, information-psychological effect, social networks

I. Введение

Ускоренное развитие вычислительной техники и новых информационно-коммуникационных технологий (ИКТ) ведет к все более серьезным изменениям в политической, экономической и социально-культурной сферах.

Под информационно-коммуникационными технологиями понимаются процессы и методы взаимодействия с информацией, которые осуществляются с применением устройств вычислительной техники и средств телекоммуникации. ИКТ-угрозы включают: хакерство и хактивизм; вывод сервера из строя; хищение и шпионаж; саботаж и разрушение; стратегические атаки и информационное противоборство; вредоносное информационно-психологическое воздействие; вмешательство во внутренние дела государства с использованием ИКТ; использование ИКТ-средств в террористических и экстремистских целях.

Сегодня мир живет в условиях четвертой индустриальной революции, объединяющей возможности промышленного производства, информационных технологий, интернета вещей и услуг. Индекс конкурентоспособности экономики государств сильно и устойчиво коррелирует с индексом развития ИКТ.¹ По оценкам Бостонской консалтинговой группы, влияние Интернета на эффективность деятельности фирм и предприятий выше, чем воздействие любой другой технологии со времен предыдущей промышленной революции.² Таким образом, развитие ИКТ-средств ведет к прорывным результатам не только в виртуальном, но и во вполне реальном, физическом пространстве. Вероятно, поэтому сегодня идет жесткая борьба за роли в рамках четвертой индустриальной революции и за ее результаты.

В ходе этой борьбы стремительное нарастание угроз и разногласий между государствами в ИКТ-сфере сделало информационное пространство ареной глобального конфликта. Следовательно, возникла ситуация, когда это пространство должно также стать территорией необходимого и неизбежного сотрудничества. Осознание Россией этого факта привело к тому, что в конце XX в. РФ стала инициатором международного обсуждения соответствующих проблем. С

тех пор активность России в сфере обеспечения международной информационной безопасности (МИБ) в рамках ООН и других организаций направлена на выработку подходов к управлению ИКТ-пространством, а впоследствии – и к контролю над ним и в итоге – на установление международного правового режима для создания эффективной системы информационной безопасности.

Однако процесс разработки режима обеспечения МИБ идет медленнее, чем множатся и нарастают угрозы в данной сфере. Поиск компромисса в ходе переговоров на многосторонней основе – единственный способ минимизировать международные ИКТ-угрозы. Для этого надо прийти к общему пониманию таких угроз и рисков. Необходимость классификации ИКТ-угроз является одной из важнейших задач, зафиксированных в документах ООН, но пока еще не реализованных. В настоящее время существуют различные варианты классификации ИКТ-угроз в национальных нормативно-правовых базах тех или иных государств и организаций. Однако ни один из них пока не стал общепринятым и удовлетворяющим интересам всех заинтересованных стран. Поэтому значимость постоянного мониторинга и исследования вредоносных информационных технологий неуклонно возрастает. Данная статья базируется на анализе международного опыта в этой сфере и на той классификации угроз, которая представлена в документах РФ.

В российской нормативно-правовой базе под международной информационной безопасностью (МИБ) понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.³ В качестве одной из самых опасных угроз МИБ в российских документах указано применение информационного оружия в военно-политических целях для осуществления враждебных действий и актов агрессии. Важнейшими также признаны угрозы:

- деструктивного воздействия на элементы критически важных объектов государственной, в т. ч. информационной, инфраструктуры;
- применения ИКТ в террористических целях;
- использования ИКТ для совершения преступлений, связанных с неправомерным доступом к информации и задействованием вредоносных компьютерных программ;
- вмешательства во внутренние дела суверенного государства посредством ИКТ;
- использования ИКТ для нарушения общественной стабильности, разжигания межэтнической, межнациональной розни.⁴

Все эти вызовы представляют угрозу международному миру и требуют незамедлительного поиска дополнительных механизмов международного управления и контроля. Одним из них может стать выработка под эгидой ООН правил поведения государств при обеспечении МИБ,⁵ принятия которых добивается Россия.

II. Угроза применения ИКТ в целях осуществления враждебных действий и актов агрессии

Угроза применения ИКТ во враждебных и агрессивных военно-политических целях представляется особо острой в силу того, что в современном мире информационные операции предоставляют уникальные возможности для создания

деструктивного эффекта. Военные средства, задействованные в этих операциях, включают стратегические коммуникации, межведомственные координационные группы, действия в киберпространстве и в космосе, поддержку информации, разведку, специальные технические процедуры, процедуры электромагнитного спектра и т. д.

Бесспорным мировым лидером в этой сфере являются США. По выражению американского политолога Джозефа Ная: «Та страна, которая возглавит информационную революцию, и будет обладать большей силой по сравнению со всеми другими странами». ⁶ При этом стратегия достижения информационного превосходства (под которым в США понимается способность собирать, обрабатывать и распространять непрерывный поток информации, лишая противника возможности осуществлять подобные действия) ⁷ совершенствуется уже несколько десятилетий, что нашло отражение в доктринальных документах и в практике применения информационных операций. Это, в свою очередь, несет в себе дополнительные риски, которые снижают уровень стратегической стабильности и требует особого внимания специалистов.

Защищенность ИКТ-систем имеет стратегическое значение для большинства стран мира. Эти системы стали важным фактором обеспечения суверенитета, обороноспособности и безопасности государств. Между тем, на современном этапе речь идет об угрозе развития так называемых информационных вооружений. По некоторым оценкам, уже более 30 государств обладают наступательным кибернетическим оружием (кибероружием). ⁸ Применение ИКТ может спровоцировать развязывание межгосударственного военного конфликта, в первую очередь, из-за опасности несоразмерного реагирования на такие угрозы и атаки: в ответ пострадавшая сторона может применить реальное оружие. Кроме того, конфликт может возникнуть по ошибке, поскольку в настоящее время отсутствует универсальная методология идентификации нарушителей, не выработаны критерии квалификации кибератак как вооруженного нападения, не сформированы универсальные принципы расследования инцидентов. Ситуацию только усугубило решение НАТО о применении статьи 5 устава альянса в ответ на кибернападения.

На сегодняшний день в мире создан широкий спектр ИКТ-средств для применения в военной области. Они включают:

- *борьбу с системами управления и контроля* — военную стратегию с применением информационной среды на поле боя для физического разрушения командной структуры противника;

- *разведывательное противоборство* — наступательные и оборонительные операции с использованием автоматизированных систем, которые, в свою очередь, являются потенциальными объектами кибератак;

- *электронное противоборство* — военные действия с использованием электромагнитной и направленной энергии для контроля над противником. Эти действия имеют три разновидности: электронная атака, электронная защита и поддержка электронного противоборства. ⁹ В источниках и терминологии на русском языке эквивалентом понятия «электронное противоборство» часто является «радиоэлектронная борьба» (РЭБ); ¹⁰

- *военные средства, способствующие проведению информационных операций*. Они, в частности, включают стратегические коммуникации, вмешательство в киберпространстве и космосе, военную информационную поддержку, разведку, совместные операции электромагнитного спектра и т. д.

Возникающие в связи с использованием этих средств проблемы можно отнести к различным элементам военной организации и инфраструктуры.

Важнейшим из них является блок киберугроз в сфере ядерного оружия (ЯО). Существуют различные точки зрения относительно вероятности и последствий вредоносного воздействия ИКТ-средств на системы командования, управления и контроля над ЯО: от полного отрицания такой угрозы до мнения о резком росте ее вероятности. Однако в военной стратегии необходимо исходить из худших сценариев развития событий. Следовательно, данная проблема должна находиться в фокусе внимания ученых и практиков, в первую очередь, из государств-обладателей ЯО. При этом речь не идет о необходимости в корне менять основополагающие принципы управления ЯО. Киберугрозы лишь обостряют, осложняют, углубляют, усиливают и видоизменяют те проблемы, которые и так всегда существовали в обеспечении безопасности ЯО.

Одной из самых серьезных угроз в военной ядерной сфере является возможность влияния ИКТ на вероятность несанкционированного запуска баллистических ракет (БР) и на принятие решения о применении ЯО. Задача защиты БР от несанкционированных пусков возникла с момента создания первых ракет. Она каждый раз решается заново при создании новых БР, постановке их на дежурство, подготовке и проведении испытательных, учебно-боевых и контрольно-боевых пусков. За десятилетия существования ЯО и в США, и в СССР (а потом в России) были случаи технических сбоев и человеческих ошибок, которые могли бы спровоцировать ядерный запуск. Избежать такой ситуации в будущем будет еще сложнее, так как задача снижения вероятности случайного запуска будет обостряться по мере перехода войск стратегического назначения в разных странах на цифровые технологии передачи информации. Так, по данным министерства обороны РФ, российские ракетные войска стратегического назначения (РВСН) полностью перейдут на цифровые технологии уже к 2020 г.¹¹

Ситуацию усугубляет возможность получения от систем предупреждения ложной информации о ракетном нападении со стороны противника. В связи с тем, что кибератаки становятся все более изощренными, растет вероятность обхода хакерами существующей системы защиты для отправки сигнала о запуске ракет. Кроме того, могут быть повреждены или разрушены каналы коммуникаций, созданы помехи в системе управления вооруженными, в т. ч. ядерными, силами, а также снижена уверенность принимающих решения военных в работоспособности систем управления, командования и контроля. Таким образом, в кризисной ситуации ИКТ-нападение может негативно повлиять на принятие решения об ответных действиях. Эти проблемы в настоящее время активно обсуждаются на Западе экспертами с глубоким знанием ядерных сил РФ и США, так что и в России игнорировать или недооценивать их нецелесообразно и опасно. Угрозы применения ИКТ в военно-политических целях для осуществления враждебных действий и актов агрессии, а также признаки наличия и возможности осуществления этих угроз представлены в *Таблице 1*.

Одной из особенностей современных международных отношений является феномен так называемой «мягкой силы», в качестве инструментов которой активно применяются средства информационно-психологического и информационно-технологического воздействия. Успешные для стратегов «мягкой силы» операции с применением ИКТ (в финансовой, организационной, материально-технической, информационной и идеологической сферах) позволяют с высокой степенью вероятности прогнозировать дальнейшее совершенствование и использование подобных методов с целью вмешательства во внутренние дела государств.

**Таблица 1. Применение ИКТ в военно-политических целях
для осуществления враждебных действий и актов агрессии**

Угроза	Признаки наличия угрозы	Возможности осуществления угрозы
Развитие информационных вооружений и кибервооружений	<ul style="list-style-type: none"> - Ускоренная милитаризация ИКТ-пространства; - включение в стратегии ряда государств ИКТ-сферы в интегрированное поле боевых действий; - наличие у 30 государств наступательного кибероружия и кибервойск; - наращивание странами НАТО возможностей для проведения наступательных и оборонительных информационных операций и киберопераций; - планы создания средств кибервойны у 140 стран; - сложность выявления автора ИКТ-атаки, возможность использования «ложного флага», проблема с определением ответственности за атаку. 	<p>ИКТ-средства для применения в военной области:</p> <ul style="list-style-type: none"> - борьба с системами управления и контроля; - разведывательное противоборство; - электронное противоборство; - военные средства, задействованные в проведении информационных операций.
Развитие ИКТ-средств для вредоносного воздействия на объекты военно-промышленного комплекса	<ul style="list-style-type: none"> - Наличие ИКТ-угроз для различных элементов военной организации и инфраструктуры. Важнейшие уязвимые элементы: стратегические вооружения, система предупреждения о ракетном нападении (СПРН), система командования и контроля над ядерным оружием, системы противоракетной и противовоздушной обороны; - рост масштабов применения в военных целях ударных роботизированных средств с дистанционным управлением, искусственного интеллекта, автоматизированных систем принятия решений, которые могут подвергаться кибератакам; - перевод войск стратегического назначения на цифровые технологии передачи информации, что делает их более уязвимыми для технических ошибок и преднамеренных кибератак. 	<ul style="list-style-type: none"> - Кибернападения на объекты военной или связанной с ней гражданской инфраструктуры; - причинение физического вреда программному обеспечению, элементной базе, линиям связи и сетям военного объекта; - нанесение дистанционного «логического» ущерба с помощью вредоносных программ, «логических бомб»¹² и т. д.; - причинение умышленного или непреднамеренного удаленного вреда через компьютерные сети (в т. ч. интернет) или в результате контакта с компьютером; - кибершпионаж и создание киберагентурных сетей; - киберсаботаж;
Снижение уровня стратегической стабильности	<p>Влияние развития ИКТ на рост вероятности:</p> <ul style="list-style-type: none"> - несанкционированного запуска баллистических ракет (БР), на принятие решения о применении ЯО; - получения ложной информации от СПРН о запуске БР со стороны противника из-за растущей изощренности кибератак; 	<ul style="list-style-type: none"> - подрыв уверенности командования и персонала в бесперебойной и эффективной работе систем.

	<ul style="list-style-type: none"> - повреждения или разрушения каналов коммуникаций, создания помех в системе управления вооруженными, в т. ч. ядерными, силами; - снижения уверенности военного командования в работоспособности систем управления и контроля над вооруженными силами; - влияние роста вероятности выведения из строя или уничтожения ЯО посредством ИКТ на будущее процессов ядерного разоружения и нераспространения; - влияние ИКТ-факторов на уровень стратегической стабильности. 	
<p>Использование «мягкой силы» с применением ИКТ во враждебных военно-политических целях, для вмешательства во внутренние дела государств</p>	<p><i>Рост количества фактов вмешательства во внутренние дела государств с применением ИКТ:</i></p> <ul style="list-style-type: none"> - «бархатная революция», Чехословакия, 1989 г.; - «бульдозерная революция», Югославия, 2000 г.; - подготовка вторжения с применением ИКТ, Афганистан, 2001 г.; - «революция роз», Грузия, 2003 г.; - вторжение с применением ИКТ, Ирак, 2003 г.; - «оранжевая революция», Украина, 2004 г.; - «революция тюльпанов», Киргизия, 2005 г.; - «жасминовая революция», Тунис, 2011 г.; - «твиттерная революция» («революция лотоса»), Египет, 2011 г.; - гражданская война, Ливия, 2011 г.; - «евромайдан», Украина, 2013–2014 гг.; - «революция розеток», Армения, 2015 г.; - гражданская война, Сирия, 2011 г. – н. вр. 	<p><i>Альтернативные военному давлению методы и средства воздействия на противника:</i></p> <ul style="list-style-type: none"> - экономические (ИКТ-воздействие на промышленные и финансовые объекты); - информационные методы и средства для подготовки и проведения массовых беспорядков, антиправительственных демонстраций, политических акций, государственных переворотов (посредством пропагандистского иновещания, интернет-поисковых систем, социальных сетей, сетевых «зеркал», мобильных приложений, смс)

Альтернативой гонке информационных вооружений могло бы стать принятие на уровне ООН предложенных Россией Правил ответственного поведения государств в области обеспечения международной информационной безопасности, открытых для присоединения любых государств на добровольной основе.

Для снижения остроты упомянутого спектра угроз, в частности, целесообразно:

– включать вопросы безопасности ИКТ в переговоры по ядерным вооружениям и стратегической стабильности на двусторонней (РФ–США, РФ–КНР) и многосторонней основе с участием России;

- продолжать инициативную деятельность России по созданию международного режима информационной безопасности под контролем ООН, включая принятие Правил ответственного поведения государств в области обеспечения международной информационной безопасности, разработку международных норм по средствам и методам предотвращения и устранения киберконфликтов, развитие международных мер укрепления доверия в сфере ИКТ;
- продолжать деятельность России по инициированию международных переговоров о мерах предотвращения инцидентов в ИКТ-пространстве, подходах к отграничению зон ответственности государств в ИКТ-среде и создании международного органа по информационным спорам;
- государствам с ЯО: совершенствовать информационную безопасность критически важной государственной инфраструктуры, военных объектов; повышать эффективность подготовки персонала (унификация, территориальное распределение, дублирование обработки данных, узкая специализация ПО и т. д.); обеспечивать боевую устойчивость стратегических сил сдерживания в условиях возможной деградации объектов критической инфраструктуры;
- расширять международные исследовательские проекты с участием российского научно-экспертного сообщества для обсуждения проблем организации партнерства в области международной информационной безопасности (МИБ);
- расширять участие российского научно-экспертного сообщества в процессе принятия государственных решений по проблемам ИКТ-пространства:
 - способствуя развитию теоретических, методологических и прогностических исследований проблемы стратегической стабильности с учетом дестабилизирующих ИКТ-факторов;
 - развивая на базе научно-экспертного сообщества международное сотрудничество с целью консолидации усилий мирового сообщества для совместного противодействия ИКТ-угрозам и формирования общего видения современных угроз в информационной сфере;
 - развивая национальные и международные научные исследования механизмов и способов противодействия угрозам МИБ и создавая, таким образом, условия для прогрессивного развития международного права в ИКТ-области;
- расширять национальные и международные исследования по систематизации анализа данных об инцидентах в ИКТ-среде и атрибуции государств, ответственных за возникновение инцидентов.

III. Деструктивное воздействие ИКТ на критически важные объекты государственной инфраструктуры

К критически важным объектам инфраструктуры государства относят системы и средства, бесперебойное функционирование которых настолько жизненно важно для страны и ее населения, что нарушение их работы или их уничтожение оказывает необратимое негативное воздействие на национальную и экономическую безопасность, здравоохранение, правопорядок и т. д. Среди общемировых тенденций, повышающих риски для критически важных объектов:

- использование личных мобильных устройств на таких объектах;
- переход на цифровые системы управления производственными и технологическими процессами;
- подключение офисных и промышленных корпоративных сетей объектов инфраструктуры к интернету;

– сложность трансконтинентальных цепочек поставок программного обеспечения систем управления производственными и технологическими процессами.

Эти тенденции касаются систем органов государственной власти, банковской деятельности, спутниковых, нефтегазовых систем, ядерных и военных объектов. Наибольшее беспокойство вызывает то, что в военной сфере под угрозой оказываются системы командования и управления ядерным оружием.

Одна из первых известных кибератак произошла еще до появления интернета – в 1982 г. в СССР. Тогда группа хакеров установила «троян» в контролируемую работу сибирского нефтепровода SCADA-систему, что привело к мощному взрыву. О том, что эта атака была организована ЦРУ США, стало известно только в 2004 г., когда бывший секретарь министерства обороны США и советник президента Р.Рейгана Томас Рид опубликовал свою книгу “At the Abyss: An Insider’s History of the Cold War”.¹³

С тех пор произошло огромное число кибернападений на критическую инфраструктуру (КИ). В настоящее время более 30 стран обладают программным обеспечением для организации таких нападений. При этом средний ущерб от целевой кибератаки на КИ составляет 1,7 млн. долл. США, а средний размер потерь промышленной компании от кибератак – более 0,5 млн. долл. в год.¹⁴ Растущая сложность оборудования и КИ ведет к росту вероятности ошибок и уязвимостей, что может быть использовано противником.

Яркой иллюстрацией масштаба и характера подобных угроз уже в XXI в. стало целенаправленное вредоносное воздействие на физические объекты критически важной инфраструктуры Ирана в 2010–2012 гг. с применением ИКТ (посредством кибернетического воздействия). Применение этих уникальных кибертехнологий стало важным инструментом влияния на изменение внутренней и внешней политики Ирана, дополняющим и не уступающим по силе воздействия политическим и экономическим санкциям и даже военным мерам. По целому ряду критериев специалисты из разных стран оценивают этот инцидент как первый и пока единственный пример применения кибероружия.

Речь идет об использовании ВП “Stuxnet”, “Duqu”, “Wiper”, “Flame” и др. в качестве инструмента для проведения комплексных массированных кибератак, осуществленных, в частности, против предприятий мирной ядерной энергетики Ирана: АЭС в г. Бушер и завода по обогащению урана в г. Натанз, а также объектов нефтеперерабатывающей промышленности.¹⁵ Эти вредоносные программы были обнаружены специалистами из разных стран в 2010–2012 гг.¹⁶ Их объединяет ряд общих технических параметров, высокая сложность кода и цели атаки. Программисты отмечают, что функционалы этих ВП отличаются от привычных параметров, используемых в сфере киберпреступности ВП: обнаруженные в Иране вредоносные программы «были созданы не для хищения денежных средств и индивидуальных данных пользователя, не для рассылки спама, а в целях вредительства на предприятиях и выведения из строя промышленных систем».¹⁷ При комплексных атаках на объекты Ирана использовался целый комплекс новейших уникальных ВП для достижения разных целей. Так, вредоносная программа “Stuxnet” предназначалась для вывода из строя промышленного оборудования, ВП “Duqu” – для шпионажа за иранской ядерной программой,¹⁸ ВП “Wiper” – для уничтожения конфиденциальных данных с жестких дисков компьютеров правительства и министерства нефти Ирана,¹⁹ ВП “Flame” (“Flamer”) – для хищения данных и организации массовой слежки, в т. ч. на территории секретных объектов, ВП “Gauss” – для шпионажа и хищения

финансовой информации, ВП “MiniFlame” – в качестве «инструмента для хирургически точных атак» с целью хищения данных.²⁰

Обнародованный российской IT-компанией «Лаборатория Касперского» анализ содержит вывод о том, что над созданием всех этих вредоносных компьютерных программ работала либо одна группа разработчиков, либо сотрудничающие команды высоко квалифицированных профессионалов, обладающих значительными финансовыми средствами и мощными техническими и иными ресурсами, что возможно только при поддержке государственных структур.²¹ Поэтому комплексные кибератаки на критически важные объекты государственной инфраструктуры Ирана рассматриваются специалистами не просто как пример киберпреступности, а как кибервойна. Соответственно, применявшиеся при этом средства относятся к кибероружию – созданным и профинансированным государственными структурами ВП, которые могут применяться против граждан, важных стратегических объектов, организаций и государственных ведомств. Использование таких ВП способно привести к реальной войне. Генеральный директор Лаборатории Касперского Е.Касперский сравнил факты применения ИКТ в Иране с открытием «ящика Пандоры».²² У многих экспертов нет сомнений в том, что за этой кибервойной стоят США и Израиль,²³ хотя до сих пор прямых доказательств этого нет. Сложность атрибуции препятствует установлению источника атак извне, а направленность подобных действий против государства и сопутствующие политические риски препятствуют признанию факта кибератаки как атакующей, так зачастую и потерпевшей сторонами.

Некоторые из этих ВП применялись и позднее. В настоящее время уже существует целый класс программного обеспечения (ПО), которое квалифицируется как кибероружие. Разрабатывается и применяется новое вредоносное ПО, на обнаружение которого могут уйти многие годы.

Результаты кибернетической войны против Ирана, доказавшие эффективность применения кибероружия, позволяют прогнозировать ускоренную разработку и использование такого оружия одними государствами против других в будущем. В настоящее время источники ВП существуют во многих странах, однако 83% всех используемых для распространения вредоносного ПО площадок расположены всего в десяти странах. Лидером в данной области являются США, где находится четверть всех источников заражения.²⁴ Подобные системы могут использоваться против нефтепроводов, электро- и атомных станций, коммуникационных систем, портов, аэропортов и даже военных установок, что может привести к тяжелым последствиям как на государственном, так и на международном уровнях. Таким образом, эти средства представляют собой перспективное стратегическое оружие.

По данным Лаборатории Касперского, Россия в течение нескольких последних лет входила в десятку стран, чаще других подвергавшихся кибернападениям на компьютеры промышленных объектов.²⁵ Несмотря на то, что в абсолютном выражении число таких кибератак растет с каждым годом, в процентном отношении (по сравнению с другими странами) ситуация в последние два года улучшилась.

По данным на июль 2018 г. в число стран, в которых процент атакованных компьютеров промышленных объектов оказался особенно высоким, вошли Индонезия (50,6%), Вьетнам (46,8%), Алжир (46,8%), Марокко (45,5%), Китай (40%), Индия (35,3%), Мексика (30,5%), Перу (30,2%), ОАЭ (29,4%) и Иран (29%).²⁶ При этом средние годовые убытки от кибератак на предприятиях с численностью более

500 сотрудников достигали 497000 долл. США.²⁷ Процент атакованных компьютеров на промышленных объектах от всего числа атакованных компьютеров в мире компьютеров составлял 21,3%.²⁸

Угрозы, создающие проблему кибербезопасности критически важных объектов государственной инфраструктуры, а также признаки наличия и возможности осуществления этих угроз представлены в *Таблице 2*.

Таблица 2. Проблема деструктивного ИКТ-воздействия на элементы критически важных объектов государственной, в т. ч. информационной, инфраструктуры

Угроза	Признаки наличия угрозы	Возможности осуществления угрозы
Развитие ИКТ-средств для нападений на критическую инфраструктуру у государств	<ul style="list-style-type: none"> - Более 30 стран обладают программным обеспечением (ПО) для нападения на объекты КИ; - показатель опасности для автоматизированных систем управления технологическими процессами – критический или высокий;²⁹ - средний ущерб от целевой кибератаки на КИ составляет 1,7 млн. долл. США;³⁰ - потери промышленной компании от кибератак составляют более 0,5 млн долл. в год;³¹ - в 2017 г. связанные с вредоносным ПО инциденты возникали у примерно 40% госучреждений в мире; - на государственные ресурсы РФ совершается более 70 млн. кибератак в год;³² - ежемесячно в 2017 г. кибератаки совершались на каждый четвертый компьютер на промышленных предприятиях РФ;³³ - растущая сложность оборудования и ПО КИ ведет к росту вероятности ошибок и возникновения уязвимостей, что может быть использовано противником. 	<ul style="list-style-type: none"> - Кибертерроризм и атаки, организованные госструктурами; - кибершпионаж; - хактивизм; - DDoS-атаки³⁴ на КИ; - атаки вредоносного ПО; - блокировщики и шифровальщики (программы-вымогатели); - атаки на портативные и мобильные устройства; - инциденты из-за ошибок сотрудников; - целевые кибератаки с помощью компьютерных вредоносных программ; - сетевые кибератаки; - подключение нежелательных устройств; - неавторизованные соединения с сетями Wi-Fi; - неавторизованные сетевые устройства и коммуникации в индустриальной сети; - разработка и применение нового вредоносного ПО, на обнаружение которого могут уйти годы.
	<p>Ускоренный рост числа кибератак на КИ:</p> <ul style="list-style-type: none"> - Сибирский нефтепровод, СССР, 1982 г.; - нефтяная компания "Chevron", США, 1992 г.; - система водоснабжения "Salt River Project", США, 1994 г.; - Газпром, РФ, 1999 г.; - система водоснабжения "Maroochy Water System", Австралия, 2000 г.; - нефтяная компания "PDVSA", Венесуэла, 2002 г.; - интернет-инфраструктура Эстонии, 2007 г.; - первое применение кибероружия: массированные целевые комплексные кибератаки на ядерный комплекс, Иран, 2010–2012 гг.; - нефтяная компания "Saudi Aramco", Саудовская Аравия, 2012 г.; - АЭС "Monju", Япония, 2014 г.; - компания «Прикарпатьеоблэнерго», Украина, 2015 г.; 	

	<ul style="list-style-type: none"> - АЭС, ФРГ, 2016 г.; - судоходная компания "Maersk", Дания, 2017 г.; - кредитная компания "Equifax Inc.", США, 2017 г.; - Национальная система здравоохранения, Великобритания, 2017 г.; - министерство энергетики и угольной промышленности, Украина, 2018 г.; - Роскомнадзор, РФ, 2018 г. 	
--	--	--

Анализ указанных угроз приводит к выводу о том, что глобальная цель обеспечения информационной безопасности уже носит стратегический характер. Одним из важнейших направлений политики России по минимизации таких угроз должно стать совершенствование эффективности системы сертификации импортных программных средств и элементной базы, планируемых для применения на объектах, критически важных для обороны и безопасности страны. В совершенствовании также нуждается система обеспечения информационной безопасности разрабатываемых современных компьютерных технологий в условиях расширения импортозамещения программно-аппаратных компонентов программного обеспечения и оборудования с целью полного перехода на отечественную элементную базу в обозримой перспективе.

IV. Угроза интернет-пропаганды и интернет-рекрутинга со стороны террористов и экстремистов

Современные угрозы информационной безопасности лежат и в технологической, и в политико-психологической сферах. При этом провести четкое разграничение между ними бывает достаточно сложно. Для выявления признаков наличия той или иной угрозы необходим глубокий профессиональный анализ в обеих областях.

Так, например, проблема интернет-пропаганды и интернет-рекрутинга со стороны террористов и экстремистов имеет и технологический, и психологический аспекты. Вербовка в сетевые сообщества экстремистского и террористического типа проводится с применением специально разработанной системы мер, в т. ч. высокотехнологических, по выявлению в различных интернет-группах лиц, склонных к активной или пассивной поддержке соответствующих взглядов и действий, с целью дальнейшего вовлечения таких лиц в свои ряды. Психологические угрозы, таким образом, выражаются в возможности воздействовать через информацию в интернете на разум и психику человека и, прежде всего, молодежи. Они также включают распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде общества, об использовании ИКТ для вмешательства во внутренние дела суверенного государства.³⁵

Эти угрозы исходят из возможности применения социальных сетей в качестве инструмента информационно-психологического воздействия, пользуясь тем, что люди публикуют в сети информацию о себе, круге своего общения, своих интересах, объединяются в сообщества по интересам и ведут публичное общение на разные темы. Кроме того, существуют широкие возможности по распространению визуальных и аудиовизуальных материалов, а также поиску пользователей в сети по определенным параметрам (возраст, пол, место

проживания, образовательное учреждение, политические взгляды, вероисповедание и т. п.). Социальные сети становятся площадкой для осуществления вредоносного воздействия, поскольку обладают рядом свойств, делающих их уязвимыми к действиям преступников, включая:

- возможность создания учетных записей вымышленных персонажей, осложняющая идентификацию пользователя;
- несовершенство системы контроля над информацией в сетях: часто пользователи не соблюдают те правила, которые обязываются соблюдать при регистрации;
- возможность злоупотребления правом на конфиденциальность переписки в преступных целях;
- широкие возможности для умышленной дезинформации населения путем «вброса» искаженных, недостоверных данных из сомнительных источников.

Помимо возможности оказывать целенаправленное влияние через социальные сети, с т. ч. в целях радикализации, пропаганды экстремистских идей и рекрутинга в состав незаконных группировок, интернет дает и другие уникальные возможности для осуществления широкомасштабного дистанционного воздействия. При этом речь идет об одновременном влиянии на такую широкую аудиторию, которую невозможно физически собрать в одном месте. Таким образом, интернет исключительно эффективен для осуществления информационно-психологического воздействия как комплекса психологических операций с помощью специально подготовленной информации, пропаганды и агитации, доводимой до объекта воздействия различными способами. Это касается любого воздействия, включая размещение в открытом доступе экстремистской и террористической информации.

Кроме того, серьезную опасность представляют случаи размещения информации, не носящей открытого противоправного характера, но при этом имеющей признаки вредоносного воздействия. Примером могут служить попытки манипулирования общественным сознанием в различных целях, формах и с использованием различных методов: от простого высказывания до сложных многоходовых схем, разработанных группами профессионалов для ведения целенаправленной разрушительной пропагандистской работы. При этом пропаганда экстремизма и терроризма в настоящее время происходит в соответствии с маркетинговыми правилами продвижения на рынок нового товара, с задействованием всех современных пиар-, медиа- и политических технологий. Так, для реализации информационно-коммуникационной политики запрещенной в России террористической организации «Исламское государство» (ИГ) была создана серьезная медиаинфраструктура. Она включала центр «Аль-Фуркан» для производства широкого спектра медиапродукции (фильмов, аудио- и видеоматериалов, брошюр, информационных материалов) для распространения в интернете; медиафонд «Айнад» для распространения джихадистских проповедей и песнопений (*нашидов*), продвигаемых онлайн через подконтрольные ИГ сайты и соцсети; медиа-агентство «Итисаам» для производства и распространения экстремистского контента на арабском языке; медиацентр «Аль-Хайят», ориентированный на немусульманскую, прежде всего, западную аудиторию и распространение материалов на 24 языках, в т. ч. английском, немецком, русском и французском.³⁶

Разрушительная работа террористов в интернете, включая создание собственных программных разработок, достигла достаточно высокого уровня.

Статистика показывает, что в настоящее время использование интернета в таких вредоносных целях приобретает глобальные масштабы по всему миру.

Выявленные случаи вербовки в состав экстремистских и террористических организаций молодых людей из разных стран (среди которых достаточно много студентов, образованной и благополучной молодежи и даже детей) поставили новые вопросы перед обществом и государством. Каков порядок привлечения молодежи в экстремистские и террористические организации? Какие методы применяются вербовщиками для вовлечения новых членов? В чем мотивация тех, кто становится жертвой интернет-рекрутинга? И, наконец, самый главный вопрос: как противодействовать этим явлениям?

Для того, чтобы изучать вопросы подготовки и развития таких действий в информационном пространстве, чтобы распознавать их на ранних стадиях и организовать эффективное противодействие им, необходимо совершенствовать комплексную систему контроля оперативной обстановки в интернете. Для минимизации угрозы, в частности, целесообразно:

- оперативно выявлять в социальных сетях информацию, наносящую вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде;
- повышать уровень информированности населения об опасности информационно-психологического воздействия, в частности, об угрозе вербовки в террористические организации через интернет;
- создавать достоверные, надежные, актуальные ресурсы информации о методах вербовки в интернете;
- интегрировать молодежь в общественно-полезную деятельность для противодействия призывам к совершению противоправных деяний в социальных сетях и ведению пропаганды;
- проводить мониторинг страниц, имеющих аудиторию более 3000 человек в социальных сетях, на предмет достоверности размещаемой информации и отсутствия признаков информационно-психологического воздействия;
- с учетом трансграничности угрозы вредоносного использования интернета, развивать международное сотрудничество на уровне ООН, региональных организаций и на двусторонней основе, совершенствовать нормативно-правовую базу в этой области;
- развивать сотрудничество в разработке и усовершенствовании технических средств для выявления противоправной информации в социальных сетях.

V. Заключение

Анализ угроз, указанных в официальных документах РФ и в международных документах по проблематике информационной безопасности, выводит на осознание еще одного блока проблем, связанных с необходимостью усовершенствования механизма принятия государственных решений по минимизации и предотвращению соответствующих рисков в информационном пространстве. Практически на любом этапе процесса принятия государственных решений в этой сфере не обойтись без особенно ценной роли экспертного сообщества, основой которого являются научные и образовательные учреждения (обеспечивающие начальное и среднее образование, высшее профессиональное образование, профессиональную переподготовку и т. д.). Деятельность образовательных учреждений должна быть направлена и на подготовку

специалистов по выявлению противоправной деятельности в ИКТ-пространстве и профилактику в отношении потенциальных жертв такой деятельности.

В России на уровне средней школы уже в течение многих лет ведется подготовка детей по информатике и программированию. Результаты этой работы можно оценить по тем высоким и призовым местам, которые российские школьники ежегодно занимают на международных олимпиадах по соответствующим предметам.

Задачи учреждений по переподготовке кадров и повышению квалификации ясны: это образовательный процесс для руководителей и специалистов в области информационной безопасности (ИБ) для федеральных, региональных, муниципальных органов управления и хозяйствующих (коммерческих) структур.

Чтобы оценить эффективность высшего профессионального образования в рассматриваемой области, целесообразно выделить ключевые особенности современной системы обеспечения безопасности в информационном пространстве. К ним, в частности, относятся:

- ускоренное нарастание угроз в ИКТ-пространстве;
- отставание теории (научной, интеллектуально-политической и нормативно-правовой) в сфере информационной безопасности от практики. С этим связано и недостаточное развитие соответствующих международных механизмов контроля над разрушительными информационными технологиями. Такое положение вещей пока не позволяет говорить о возможности применения хорошо разработанной теории к практике;
- недостаток специалистов. Еще совсем недавно казалось, что для решения существующих проблем вполне достаточно так называемых «безопасников» (жарг.) – в основном программистов и, в основном, в специальных структурах. Однако нарастание проблем доказывает, что это не так;
- выход проблемы обеспечения информационной безопасности на международный уровень:
 - в рамках двусторонних межгосударственных отношений;
 - в рамках международных организаций;
 - в рамках ООН (при инициативной роли России).

Эти особенности также выводят проблему обеспечения международной информационной безопасности на меж- и мультидисциплинарный уровни и подчеркивают необходимость разработки новой стратегии подготовки специалистов по безопасности в информационном пространстве. При этом важно находить дополнительные механизмы мотивации студентов к разработке новых подходов, методик и стратегий в этой области.

Высшее профессиональное образование по различным направлениям информационной безопасности предоставляется более чем в 170 российских вузах разной ведомственной принадлежности, среди которых 35% – это гражданские учебные заведения.³⁷ Факультеты или кафедры по подготовке таких специалистов, в частности, существуют в МГУ им. М.В.Ломоносова, Санкт-Петербургском государственном университете, МГТУ им. Баумана, МИФИ, МАИ, МГИМО, РГГУ и даже в Московской духовной академии. Однако того числа специалистов (как технических специалистов, так и юристов и международников), которые готовятся и выпускаются сейчас недостаточно.

Кроме того, качество образования в этой сфере зачастую не соответствует современным требованиям. Серьезная проблема заключается в том, что профессиональная подготовка в этой области на практике не носит междисциплинарного и мультидисциплинарного характера, тогда как от

соответствующих специалистов требуются знания и навыки на пересечении самых разных областей знаний: информационных технологий, юриспруденции, политологии, международных отношений, психологии, криминалистики и т. п. Однако в настоящее время выпускники технических вузов зачастую не владеют знаниями, позволяющими понимать политическую составляющую проблемы обеспечения информационной безопасности. В свою очередь, специалисты-международники, занимающиеся информационной безопасностью, должны не только иметь соответствующие знания и навыки в области международных отношений и дипломатии, но и понимать специфику угроз в технологической сфере, владеть научными методами исследования проблем ИБ и т. д. Кроме того, несмотря на наблюдающийся в России переизбыток будущих юристов, специалистов по правовым отношениям в информационной сфере также не хватает.

В целом, высококвалифицированных кадров в сфере обеспечения МИБ остро не хватает (причем далеко не только в России), нет достаточной теоретической и методологической базы, а процесс принятия решений в этой области недостаточно эффективен. Как следствие, на фоне продолжающегося ускоренного нарастания угроз пока отсутствует международная стратегия реакции на эти угрозы, их предотвращения и т. д. Проблемы, связанные с образованием в этой сфере, имеют место во многих странах, носят глобальный характер и требуют совместных действий на международном уровне. Безусловно, их разрешение является длительным процессом, и все же эта цель достижима, подобно тому, как это происходило с подготовкой специалистов для решения других глобальных мультидисциплинарных проблем.

Исходя из особенностей ИКТ-пространства, перед научно-экспертным сообществом и научно-исследовательскими организациями на современном этапе стоят особые, новые задачи.

1. Разработка теории и методологии обеспечения безопасности информационного пространства (в т. ч. развитие и совершенствование понятийного аппарата). Примером могут служить доклады РЭНД-корпорации (США) 1996 и 1998 гг.,³⁸ которые стали теоретической и практической базой американской политики в этой сфере.

2. Разъяснение и доведение до более широкого круга экспертов сути проблем безопасности в информационном пространстве, которая, в частности, отражена в таких документах, как комплекс резолюций ООН на тему «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», а также результатов деятельности Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, правил поведения в области МИБ и т. д.

3. Постоянный мониторинг инцидентов и разносторонний анализ практических примеров нарушения информационной безопасности для создания базовой теории, методов ее применения на практике и ее дальнейшего совершенствования.

4. Анализ долгосрочных тенденций развития информационного пространства, разработка инновационных идей по управлению в сфере МИБ.

5. Подготовка материалов для отстаивания государственных интересов России в сфере МИБ.

6. Меж- и мультидисциплинарные исследования проблем обеспечения безопасности в глобальном информационном пространстве.

7. Внедрение и распространение культуры использования информационного пространства.

8. Выработка механизмов противодействия интернет-рекрутингу и интернет-пропаганде со стороны экстремистских и террористических акторов.

9. Исследование проблем обеспечения информационно-психологической безопасности личности и общества от деструктивных воздействий интернета и других информационных источников.

10. Участие в разработке стратегии подготовки соответствующих специалистов в высших учебных заведениях.

11. Разработка эффективных методов научного прогнозирования и планирования в сфере ИКТ, что не осуществимо в рамках лишь какой-то одной научной дисциплины или направления.

12. Поиск вариантов совмещения интересов разных государств в процессе разработки универсального режима безопасности в информационном пространстве и нераспространения информационного оружия.

13. Активизация участия российского научно-экспертного сообщества в процессе принятия государственных решений по проблемам ИКТ-сферы, в т. ч.:

- способствование развитию теоретических, методологических и прогностических исследований проблемы стратегической стабильности с учетом дестабилизирующих ИКТ-факторов;

- развитие международного сотрудничества на базе научно-экспертного сообщества с целью консолидации усилий для совместного противодействия угрозам МИБ и формирования общего видения современных угроз в информационной сфере;

- развитие национальных и международных научных исследований механизмов и способов противодействия угрозам МИБ, создание условий для последовательного развития международного права в ИКТ-области;

- расширение национальных и международных исследований по систематизации анализа данных об инцидентах в ИКТ-среде и идентификации государств, ответственных за возникновение инцидентов.

14. Организация в России образовательного центра информационной безопасности для граждан государств СНГ, Организации Договора о коллективной безопасности (ОДКБ), Шанхайской организации сотрудничества (ШОС), группы БРИКС (Бразилии, России, Индии, Китая и ЮАР). Такой центр должен быть нацелен на предоставление обучающимся всесторонней и ориентированной на политические аспекты программы овладения знаниями об актуальных угрозах в ИКТ-сфере и методами разработки и принятия решений в области информационной политики, стратегии и планирования. Учебные программы курсов Центра должны способствовать подготовке общей стратегии противодействия угрозам МИБ.

При этом важно постепенно решать и существующую в настоящее время в научной среде проблему обособленности, когда часть учреждений и организаций занимается решением информационно-технологических проблем, часть – информационно-психологических, часть – правовых и т. д. Необходима более тесная координация их действий в целях комплексного применения экономических, технических, военных и политических механизмов для решения проблем в сфере международной информационной безопасности.

ПРИМЕЧАНИЯ

¹ Schwab K. The fourth industrial revolution: what it means and how to respond? // The Fourth Industrial Revolution: A Davos Reader. Foreign Affairs Special Collection. January 2016. P. 3–11. См. также онлайн-версию: URL: <https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution>

² The economic impact of shutting down Internet and mobile phone services in Egypt. Organization for Economic Cooperation and Development (OECD) Directorate for Science, Technology and Industry. 04.02.2011. URL: <http://www.oecd.org/sti/ieconomy/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm>.

³ Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. (Утверждены Президентом Российской Федерации В.Путиным 24 июля 2013 г., № Пр-1753). URL: <http://www.scrf.gov.ru/security/information/document114>.

⁴ Doctrine of Information Security of the Russian Federation (Approved by Decree of the President of the Russian Federation No. 646 of December 5, 2016). URL: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptlCkB6BZ29/content/id/2563163; Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г.

⁵ Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. United Nations General Assembly. UN Doc. A/69/723. 13 January 2015. URL: <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf/>.

⁶ Nye J.S. The information revolution and soft power // Current History. V. 113. No. 759. 2014. P. 19-22.

⁷ Joint Vision 2010. Joint Chiefs of Staff, 2010. URL: http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4240529/FID378/pdfdocs/2010/Jv2010.pdf

⁸ Ромашкина Н.П. Стратегическая стабильность: новые вызовы инфосферы. Российский совет по международным делам (РСМД): Аналитика. 23 ноября 2017 г. URL: <http://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-stabilnost-novye-vyzovy-infosfery>.

⁹ Information Warfare. Directive TS 3600.1. – Washington D.C.: U.S. Department of Defense, 21 December 1992.

¹⁰ Российская армия получит средства РЭБ нового поколения // Медиагруппа «Звезда». 03.11.2016. URL: <http://tvzvezda.ru/news/opk/content/201611031232-3nca.htm>.

¹¹ К 2020 г. РВСН полностью перейдут на цифровые технологии передачи информации. Департамент информации и массовых коммуникаций министерства обороны РФ. 03.01.2018. URL: https://structure.mil.ru/structure/forces/strategic_rocket/news/more.htm?id=12142122%40egNews.

¹² Логическая бомба – программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий (например, несанкционированного доступа к информации, искажения или уничтожения данных).

¹³ Reed T. At the Abyss: An Insider's History of the Cold War. – N.Y.: Presidio Press, 2004.

¹⁴ Kaspersky Industrial Cybersecurity: обзор компонентов решения. – М.: АО «Лаборатория Касперского», 2017. URL: https://media.kaspersky.com/ru/enterprise-security/KICS_tech_overview_RU_A5.pdf.

¹⁵ Information Security Threats During Crisis and Conflicts of the XXI Century / Ed. by N.P.Romashkina and A.V.Zagorskii. – Moscow: IMEMO, 2016.

¹⁶ The man who found Stuxnet: Sergey Ulasen in the spotlight // Eugene Kaspersky's Blog. 02.11.2011. URL: <http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight>; Российские специалисты обнаружили на Ближнем Востоке банковский троян // Взгляд. 9 августа 2012 г.; Samekh M.-B. Lessons learned from Flame, three years later // Kaspersky Lab: Opinion. 29.05.2015. URL: <https://securelist.com/lessons-learned-from-flame-three-years-later/70149/5>; Gostev A.A. The Mystery of Duqu // Threat Post. 02.10.2010. URL: <https://threatpost.com/mystery-duqu-102011/75778>.

¹⁷ Kaspersky Lab Provides its Insights on Stuxnet Worm. Kaspersky Lab Press-Release. 24 September 2010. URL: http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm.

¹⁸ Naraine R. Duqu first spotted as “Stars” malware in Iran // Kaspersky Lab Blog. 05.11.2011. URL: http://www.securelist.com/en/blog/208193211/Duqu_First_Spotted_as_Stars_Malware_in_Iran.

¹⁹ ВП “Wiper” может быть связана с израильскими разработчиками. Она создавала и удаляла ключ реестра, ссылавшийся на службу модуля “Rahdaud64”, название которого, предположительно, образовано от имени библейского царя Давида (דָּוִד, в арабской традиции — Daud) и прилагательного Rah (רָחַ), в переводе с иврита означающего «злой, плохой, вредоносный». Information Security Threats during Crisis and Conflicts of the XXI Century. Op. cit.

²⁰ Kaspersky Lab Discovers “MiniFlame,” a New Malicious Program Designed for Highly Targeted Cyber Espionage Operations. Kaspersky Lab Press-Release. 15 October 2012. URL: https://usa.kaspersky.com/about/press-releases/2012_kaspersky-lab-discovers--miniflame--a-new-malicious-program-designed-for-highly-targeted-cyber-espionage-operations.

²¹ Kaspersky Lab Provides its Insights on Stuxnet Worm. Op. cit.

²² Подробнее см. Хроника целевых кибератак. Лаборатория Касперского: интерактивный проект. <https://apt.securelist.com/?lang=ru#!/threats>.

²³ Broad W., Markoff J., Sanger D. Israeli test on worm called crucial in Iran nuclear delay // The New York Times. 15 January 2011; Williams D. Wary of naked force, Israelis eye cyberwar on Iran // Reuters Analysis. 07.07.2009. URL: <http://www.reuters.com/article/2009/07/07/idUSLV83872>; Who's Spying on You? No Business is Safe from Cyber-Espionage. Kaspersky Lab Special Report. – Moscow: Kaspersky Lab ZAO, 2013. URL: <https://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf>.

²⁴ Malware in Q3-2010: 600 Million Attempted Infections, Stuxnet, Stolen Certificates and Exploits // Kaspersky Lab Press-Release. 17 December 2010. URL: https://www.kaspersky.com/about/press-releases/2010_malware-in-q3-2010-600-million-attempted-infections-stuxnet-stolen-certificates-and-exploits.

²⁵ Подробнее см. Kaspersky Industrial Cybersecurity: обзор компонентов решения. Ук. соч.

²⁶ Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (ICS CERT). URL: <https://ics-cert.kaspersky.ru>.

²⁷ Кибербезопасность современных промышленных систем // Abiroy.com. N.D. URL: <http://abiroy.com/blog/cybersecurity-for-modern-industrial-syst>.

²⁸ Kaspersky Lab ICS CERT. Op. cit.

²⁹ Kaspersky Industrial Cybersecurity: обзор компонентов решения. Ук. соч.

³⁰ Кибербезопасность государственных организаций. Лаборатория Касперского.

URL: <https://www.kaspersky.ru/enterprise-security/government/>.

³¹ «Лаборатория Касперского»: кибератаки на промышленные компании стоят им \$0,5 млн. в год // ТАСС. 08.06.2017. URL: <http://tass.ru/ekonomika/4324669>.

³² Кибербезопасность государственных организаций. Ук. соч.

³³ Kaspersky Industrial Cybersecurity: обзор компонентов решения. Ук. соч.

³⁴ DDoS-атака – от англ. “Distributed Denial of Service attack” – распределенная сетевая атака типа «отказ в обслуживании». Этот тип атаки использует определенные ограничения пропускной способности, которые характерны для любых сетевых ресурсов, например, инфраструктуре, которая обеспечивает условия для работы сайта компании. DDoS-атака отправляет на атакуемый веб-ресурс большое количество запросов с целью превысить способность сайта обрабатывать их все и вызвать отказ в обслуживании.
URL: <https://www.kaspersky.ru/resource-center/threats/ddos-attacks>.

³⁵ Проблемы информационной безопасности в международных военно-политических отношениях / Под ред. А.В.Загорского, Н.П.Ромашкиной. М.: – ИМЭМО РАН, 2016.

³⁶ Сундиев И.Ю., Смирнов А.А., Костин В.Н. Новое качество террористической пропаганды: медиаимперия ИГИЛ // Информационные войны. 2015. № 1(33). С. 30–36; Ломтев П. Радикальный исламизм как основное оружие ДАИШ // Международная жизнь: сайт журнала. 17.12.2016. URL: <https://interaffairs.ru/news/printable/16606>.

³⁷ Вузы России по направлению «информационная безопасность» // Учеба.ру.
URL: <https://www.ucheba.ru/for-abiturients/vuz/rossiya/information-security?s=60>.

³⁸ Molander R., Riddile A., Wilson P. Strategic Information Warfare: A New Face of War. – Santa Monica (Calif.): RAND, 1996; Molander R., Wilson P., Mussington D., Mesic R. Strategic Information Warfare Rising War. – Santa Monica: RAND, 1998.