НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МИРОВОЙ ЭКОНОМИКИ И МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ
ИМЕНИ Е.М. ПРИМАКОВА
РОССИЙСКОЙ АКАДЕМИИ НАУК

Н.П. Ромашкина
А.С. Марков
Д.В. Стефанович

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ, СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Под ред. А.В. Загорского, Н.П. Ромашкиной

Москва
ИМЭМО РАН
2020

УДК 327
ББК 66.4(0)
Ромаш 698

Рекомендовано к печати
НИС Ученого совета ИМЭМО РАН

Серия «Библиотека Национального исследовательского института
мировой экономики и международных отношений имени Е.М. Примакова»

Рецензенты:
доктор военных наук, кандидат технических наук, профессор Н.И. Турко,
доктор технических наук, профессор С.А. Петренко

Ответственные редакторы – к.и.н. А.В. Загорский, к.п.н. Н.П. Ромашкина

Гл. 1 – к.полит.н. Н.П. Ромашкина; гл. 2 – д.т.н. А.С. Марков,
гл. 3 – Д.В. Стефанович,
гл. 4 – к.полит.н. Н.П. Ромашкина, Д.В. Стефанович, д.т.н. А.С. Марков

Обложка с использованием фото Е.А. Келя

Ромаш 698
Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / Отв. ред. – А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 97 с.
ISBN 978-5-9535-0581-9
DOI:10.20542/978-5-9535-0581-9

Монография посвящена актуальным вопросам международной безопасности и стратегической стабильности в условиях ускоренного развития информационно-коммуникационных технологий. Обосновывается важность обеспечения международной информационной безопасности. Рассматриваются возможности формирования под эгидой ООН режима контроля над вооружениями, основанными на информационно-коммуникационных технологиях. Анализируются различные аспекты регулирования безопасности программных систем и использования суперкомпьютеров в контексте международной безопасности. Исследуется влияние информационно-коммуникационных технологий на стратегическую стабильность. Монография адресована специалистам в области информационно-коммуникационных технологий и международной безопасности, преподавателям, студентам и аспирантам ВУЗов, а также широкому кругу читателей.

Romashkina N.P., Markov A.S., Stefanovich D.V. International Security, Strategic Stability and Information Technologies – Moscow, IMEMO, 2020. – 97 p.
ISBN 978-5-9535-0581-9
DOI:10.20542/978-5-9535-0581-9
The monograph is devoted to topical issues of international security and strategic stability in the context of accelerated development of information and communication technologies. It justifies the importance of ensuring international information security. The monograph examines the possibility of establishing an IT-arms control regime under the UN auspices. Different aspects of regulation of software security systems and of the use of supercomputers in the context of the international information security are examined. The impact of information and communication technologies on strategic stability is analyzed. This monograph is addressed to specialists in the field of information and communication technologies and international security, university lecturers, students and graduate students of universities, as well as a wide range of readers.

Публикации ИМЭМО РАН размещаются на сайте https://www.imemo.ru

ISBN 978-5-9535-0581-9

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ

АС –	автоматизированная система
АСБУ –	автоматизированная система боевого управления
АСУ –	автоматизированные системы управления
АСУ ТП –	автоматизированные системы управления технологическим процессом
БР –	баллистическая ракета
БРИКС –	Межгосударственное объединение Бразилии, России, Индии, Китая и Южно-Африканской Республики
ВС –	вооруженные силы
ВПК –	военно-промышленный комплекс
ГА ООН –	Генеральная Ассамблея Организации Объединенных Наций
ГПЭ –	Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности
ИИ –	искусственный интеллект
ИКТ –	информационно-коммуникационные технологии
КИ –	критически важная государственная инфраструктура
МИД –	министерство иностранных дел
МИБ –	международная информационная безопасность
МО –	министерство обороны
НАТО –	Организация Североатлантического договора
НПО –	неправительственная организация
ОМУ –	оружие массового уничтожения
ООН –	Организация Объединенных Наций
ПО –	программное обеспечение
ПВО –	противовоздушная оборона
ПРО –	противоракетная оборона
РВСН –	Ракетные войска стратегического назначения РФ
РГОС	Рабочая группа ООН открытого состава по МИБ
РСМД –	ракеты средней и меньшей дальности
РЭБ –	радиоэлектронная борьба
СМИ –	средства массовой информации
СПРН –	система предупреждения о ракетном нападении
СЯС –	стратегические ядерные силы
ШОС –	Шанхайская организация сотрудничества
ЮНИДИР –	Институт ООН по исследованию проблем разоружения
ЯО –	ядерное оружие

ВВЕДЕНИЕ

Данная публикация продолжает проблематику монографий Группы проблем информационной безопасности Центра международной безопасности ИМЭМО РАН имени Е.М. Примакова «Угрозы информационной безопасности в кризисах и конфликтах XXI века» и «Проблемы информационной безопасности в международных военно-политических отношениях» и направлена на исследование наиболее актуальных и важных проблем современности, связанных с угрозами от вредоносного применения информационно-коммуникационных технологий (ИКТ), а также на поиск их решения в целях укрепления международной безопасности и защиты национальных интересов России на международной арене. Как и в предыдущих работах по этой проблематике, авторы представляют читателям обширную базу источников, следуя основным научным принципам: «Ничему не верю без доказательства и ничего не оставляю без доказательства» и «То, что принято без доказательств, может быть отвергнуто без доказательств».

Информационно-коммуникационные технологии, то есть все процессы взаимодействия с информацией, осуществляемые посредством устройств вычислительной техники и различных средств коммуникации, являются неизменным атрибутом повседневной жизни, оказывают беспрецедентное влияние на экономические и политические процессы, общественные структуры и международные отношения. В последние десятилетия ИКТ стали катализатором прогресса жизнедеятельности людей. Всеобъемлющее значение новых технологий в современном мире максимально остро обозначила пандемия коронавируса SARS-CoV-2 2019–2020 годов, когда целые отрасли экономики, науки и образования перешли в режим работы онлайн. Все государства признают значительные преимущества ИКТ, но лавинообразное нарастание угроз в этой сфере привело к глубокому осознанию того факта, что их вредоносное применение может представлять серьезную опасность для мира, международной безопасности и стратегической стабильности. Таким образом, международная информационная безопасность (МИБ) стала неотъемлемой частью глобальной безопасности. Именно поэтому различные аспекты МИБ уже более 20 лет стоят на повестке дня Первого комитета Генеральной Ассамблеи ООН, который рассматривает вопросы, связанные с угрозами миру и международной безопасности и обсуждает пути их укрепления.

В первой главе монографии представлены результаты анализа этой деятельности, исследуются возможности создания международного режима по запрещению информационного (в том числе, и кибернетического) оружия, доказывается актуальность и возрастающая важность изучения этих процессов со стороны научного сообщества. Обоснована постановка проблемы МИБ как части более широкой темы международной безопасности на фоне глобальных военно-политических вызовов. Дается прогноз перспектив обсуждения вопросов обеспечения МИБ в рамках ООН. Ставится вопрос о целесообразности разработки Стратегии информационной безопасности Российской Федерации.

Одной из важнейших основ МИБ является свод из тринадцати международных правил, норм и принципов ответственного поведения государств, рекомендованный Резолюцией Генеральной Ассамблеи ООН A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятой 11 декабря 2018 года. Подчеркивая значение этих правил, следует отметить, что основное внимание в них обращено на конкретные действия мирового сообщества в рамках жизненного цикла международных конфликтов в сфере ИКТ, в информационном и, в том числе кибернетическом пространствах, а именно в латентной и открытой фазах киберконфликта. Важность этих обсуждений, в

частности, подтверждена использованием Израилем в 2019 году летального оружия в отношении готовившихся целенаправленных враждебных компьютерных атак из сектора Газа.

В настоящее время объективные причины возможного возникновения киберконфликтов, связанные с правовым и техническим регулированием безопасности компьютерных систем, исследованы недостаточно. В первую очередь это касается программных систем, которые являются системообразующим элементом сферы ИКТ, ее продуктом и одновременно одним из главных источников нестабильности. Рассматривая их жизненный цикл и роль в процессе обеспечения МИБ, следует подчеркнуть пункты 9 и 11 указанного свода правил, норм и принципов, а именно:

- государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ;
- государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры.

Обоснованию целесообразности уточнения указанных пунктов в части исследования объективных факторов возникновения и устранения уязвимостей программ, а также связанных с ними угроз и рисков в контексте международной безопасности, посвящена вторая глава монографии. При этом важно отметить, что вопросы транспарентности действий мирового сообщества в сфере ИКТ, исключительной предпочтительности предупредительных механизмов МИБ, а также повышения доверия к безопасности программных систем путем правового и технического регулирования являются максимально актуальными и востребованными.

В настоящее время использование ИКТ превращается в один из важнейших элементов военно-политического потенциала государств, дополняющий, а иногда и заменяющий традиционные политико-дипломатические средства и вооружения. В условиях параллельно развивающихся процессов разрушения режима контроля над вооружениями и роста противоречий в отношениях «великих держав» значение военной мощи, технологий военного и двойного назначения как одного из ключевых факторов соперничества и противоборства сохраняется и даже увеличивается. Одним из новейших, наиболее сложных и дорогостоящих примеров таких технологий являются суперкомпьютеры, развитие и совершенствование которых стремительно растет и становится существенным показателем возможностей государственных и негосударственных акторов. Локомотивом прогресса в повышении вычислительной мощности суперкомпьютеров в России, США и в других странах в значительно мере являются оборонные структуры: вооруженные силы и оборонно-промышленный комплекс.

Суперкомпьютеры активно внедряются для решения ключевых задач в области безопасности:

- поддержание и модернизация ядерного арсенала в условиях отсутствия натурных испытаний;
- оптимизация процессов разработки передовых видов вооружения и военной техники путем сокращения количества испытаний, благодаря качественно новым возможностям в области моделирования;

- метеорология в глобальном масштабе, в частности, в интересах военно-морских сил, позволяющая прогнозировать состояние различных сред и планировать операции с учетом всех необходимых внешних факторов;
- планирование логистического обеспечения деятельности вооруженных сил и оборонной промышленности в обычном и экстремальном режимах.

Как представляется, во всех перечисленных областях угрозы глобальной безопасности могут быть, в частности, связаны с возможным отставанием той или иной осуществляющей стратегическое сдерживание страны в этой области. При этом угроза может реализоваться как в варианте осознания отстающей стороной негативных перспектив и попытки избежать такого сценария путем инициирования конфликта, так и в случае наличия у лидирующей стороны информации об отсутствии подобных возможностей у потенциального объекта агрессии и желания закрепить доминирование путем нанесения «безответных» ударов. Проблема влияния суперкомпьютеров на процессы международной и национальной безопасности исследуется в третьей главе данной монографии.

Вопросы вредоносного использования ИКТ в военно-политической сфере являются самыми сложными в процессе международного обсуждения. Впервые указание на угрозы МИБ применительно не только к гражданской, но и к военной сфере содержалось в резолюции Генеральной Ассамблеи ООН 54/49 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 1 декабря 1999 года. С тех пор никакие новые международные документы, нормативно ограничивающие такую вредоносную деятельность, ООН приняты не были. Поэтому информационные операции, предоставляющие уникальные возможности для создания деструктивного эффекта в военно-политической сфере, постоянно совершенствуются, разрабатываются новые ИКТ-вооружения для борьбы с системами управления и контроля, разведывательного и электронного противоборства, для использования ИКТ с целью вмешательства во внутренние дела государств, для воздействия на объекты критически важной государственной инфраструктуры (КИ), и, в частности, на объекты ВПК.

Таким образом, ИКТ могут спровоцировать развязывание межгосударственного военного конфликта. В первую очередь, из-за несоразмерного использования методов реагирования на угрозы и атаки, когда пострадавшая сторона может применить в ответ реальное оружие. Кроме того, конфликт может возникнуть по ошибке, так как в настоящее время отсутствует универсальная методология идентификации нарушителей, не выработаны критерии отнесения кибератак к вооруженному нападению, не сформированы универсальные принципы расследования инцидентов. По-прежнему не решены вопросы согласования мер, предпринимаемых в ответ на информационные операции, признанные актами применения силы. В итоге информационные войны и применение новых технологий могут стать детонатором межгосударственного военного конфликта с применением даже ядерного оружия (ЯО).

ИКТ уже оказывают влияние на стратегическую стабильность. Поэтому обеспечение глобальной безопасности и стратегической стабильности требует развития и модернизации механизмов международного управления в цифровом пространстве. При этом речь не идет о необходимости в корне менять основополагающие принципы, так как ИКТ обостряют, осложняют, углубляют и видоизменяют ранее существовавшие в этой области проблемы. Так, угрозы стратегической стабильности дополнительно усиливаются в связи с развитием новых противоспутниковых систем, ударных роботизированных средств с дистанционным управлением, возможностями автономной работы различных систем

и подсистем, автоматизированных систем принятия решений и т.д., которые могут подвергаться ИКТ-атакам, средств кибер-электромагнитной деятельности, которая активно совершенствуется в развитых странах, в первую очередь, в США. Помимо технологических дестабилизирующих факторов существует еще и психологический, который можно сформулировать как утрату страха перед ядерной войной у общества и политических элит, что потенциально существенно снижает порог применения вооружений. Опасной также является убежденность в допустимости локальной «небольшой» ядерной войны и победы в ней. При этом оценка ущерба и выработка мер противодействия существенно затруднены из-за «неосязаемости» ИКТ, сложности атрибуции источника атаки, возможности действовать под «ложным флагом», широкого спектра субъектов, применяющих вредоносные технологии: государственных и негосударственных акторов, а также хакеров-одиночек. Все это повышает уровень неопределенности и нестабильности. Анализ проблематики стратегической стабильности в эпоху ИКТ представлен в четвертой главе данной монографии.

Уникальной особенностью современной системы МИБ, позволяющей надеяться на то, что международное сотрудничество в обеспечении глобальной безопасности в конечном итоге возьмет верх, является взаимная высокая ИКТ-уязвимость многих стран мира. Во-первых, наиболее уязвимыми являются государства с наиболее развитой ИКТ-сферой. Во-вторых, при отсутствии каких бы то ни было ограничений существуют стимулы для создания и взаимного применения ИКТ в военно-политических целях для враждебных действий и актов агрессии. В-третьих, страны с наиболее развитой и поэтому уязвимой для киберкинетических воздействий техносферой, реализуют комплекс мер, направленных, с одной стороны, на минимизацию возможностей оппонентов по деструктивному, системоразрушающему воздействию на их критические инфраструктуры, а с другой – на заблаговременную скрытую подготовку глобальных систем оперативно-технических позиций (киберагентурных сетей) для контроля и реализации при необходимости аналогичных воздействий на ключевые объекты критической инфраструктуры других стран. Однако при этом для страны, являющейся лидером в сфере ИКТ-противоборства, существует серьезная опасность, связанная с риском контроля, дезинформации и манипулирования со стороны компетентного противника. Это возможно, если противник выявит киберагентурные сети страны-лидера, будет их эксплуатировать и наблюдать за их деятельностью, не затратив при этим значимых усилий, кроме действий по выявлению и отслеживанию киберактивности.

По этим причинам обеспечение международной информационной безопасности в современную цифровую эпоху становится одной из важнейших задач мирового сообщества.

ГЛАВА 1.

Международная безопасность и информационно-коммуникационные технологии

1.1. Международная информационная безопасность как часть проблемы глобальной безопасности

Лавинообразное нарастание угроз от вредоносного применения информационно-коммуникационных технологий (ИКТ) в политической, военной, экономической и социальной сферах привело к глубокому осознанию того факта, что новые технологии могут нести дополнительные опасности для международного мира и безопасности. Таким образом, проблема международной информационной безопасности, то есть 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[1], стала неотъемлемой частью международной безопасности как системы международных отношений, основанной на соблюдении всеми государствами общепризнанных принципов и норм международного права и исключающей решение спорных вопросов и разногласий между ними с помощью силы или угрозы силой, в целом. Таким образом, принципы международной безопасности, предусматривающие утверждение мирного сосуществования, обеспечение равной безопасности для всех государств, создание действенных гарантий в военной, политической, экономической и гуманитарной областях, недопущение гонки ядерных и космических вооружений, уважение суверенных прав каждого народа, справедливое политическое урегулирование международных кризисов и региональных конфликтов, безусловно, включают создание системы международной информационной безопасности. При этом под системой МИБ, предназначенной для противодействия угрозам стратегической стабильности и обеспечения равноправного партнерства в глобальной цифровой среде, понимается совокупность международных и национальных норм и институтов, главным среди которых является ООН, по регулированию деятельности различных субъектов всемирного информационного пространства[2].

Есть все основания для обсуждения проблем, связанных с развитием ИКТ, по основным направлениям деятельности ООН: мир и безопасность, права человека и устойчивое развитие. Параллельно с работой по вопросам достижений в сфере ИКТ в контексте международной безопасности в различных органах ООН идут дискуссии по другим аспектам, к которым относятся цифровое сотрудничество, управление Интернетом, устойчивое развитие и права человека (включая защиту коммерческих и персональных данных, свободу мнений и информации), а также киберпреступность и кибертерроризм.

Так как неотъемлемой частью международной безопасности является действенное функционирование закрепленного Уставом ООН механизма коллективной безопасности, проблема обеспечения МИБ стала частью повестки дня

---

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document114/.

[2] «Инфофорум-2014»: Итоги // XVI Национальный форум информационной безопасности. URL: http://2014.infoforum.ru/infoforum-2014-itogi/.

одного из шести главных комитетов Генеральной Ассамблеи ООН (ГА ООН) – Первого комитета, занимающегося вопросами разоружения и связанным и с ними вопросами международной безопасности. Именно здесь государства обсуждают угрозы миру и ищут пути его содействию. Поэтому процесс обеспечения международной информационной безопасности в ООН играет важнейшую роль и требует глубокого анализа экспертного сообщества. Можно указать целый ряд причин, обосновывающих целесообразность и важность обсуждения вопросов МИБ в Первом комитете ГА ООН. Назовем основные из них.

Во-первых, анализ и прогноз угроз от вредоносного использования ИКТ как государствами, так и негосударственными субъектами доказывает возможность влияния новых компьютерных технологий на рост вероятности реальных вооруженных конфликтов, их эскалации, а, следовательно, широкомасштабной войны. Проблема обеспечения информационной безопасности является стратегической, а уровень безопасности ИКТ оказывает значительное влияние на уровень стратегической стабильности. Речь идет об угрозе международному миру, а значит, необходим поиск дополнительных механизмов международного управления. Без согласия между государствами в этой сфере рост и масштаб таких опасностей будет возрастать. Обсуждение глобальных международных процессов в рамках Первого комитета ГА ООН позволяет разрабатывать меры по укреплению доверия, принципы и нормы ответственного поведения государств в цифровом пространстве, которые могут снизить риск вооруженных конфликтов и их эскалации. Такая деятельность позволяет акцентировать внимание и на других подходах, способствующих стабильности и безопасности в ИКТ–пространстве, таких как координация и поддержка создания потенциала безопасности информационных технологий.

Во-вторых, анализ прецедентов ИКТ–нападений на критически важную государственную инфраструктуру доказывает рост их количества и масштабов в геометрической прогрессии из года в год. Кибератаки на системы и средства, настолько жизненно важные для страны, что нарушение их работы или уничтожение оказывает необратимое негативное воздействие на национальную экономическую безопасность, здравоохранение, правопорядок, системы управления, военные объекты и т.д., напрямую угрожают жизни множества людей и обосновывают необходимость обсуждения ответственного поведения государств в информационной среде.

В-третьих, несмотря на развитие национальных и региональных инструментов регулирования и контроля деятельности в сфере ИКТ, а также в рамках международных организаций, ни одно государство в мире не может в настоящее время считать себя полностью защищенным от трансграничных информационных угроз и не способно решить связанные с этими опасностями проблемы в одиночку. Поэтому обсуждение на глобальном уровне ООН приобретает жизненно важное значение. Акцент на координации между государствами и различными заинтересованными сторонами, которые в настоящее время включены во многие национальные и региональные стратегии по кибер- и информационной безопасности, также отражаются на обсуждении этих вопросов в рамках Первого комитета ГА ООН. Результаты работы на глобальном уровне, в свою очередь, влияют на национальные и региональные нормы и принципы, что также может способствовать содействию миру и стабильности в ИКТ–пространстве.

1.2. Прошлое, настоящее и будущее международной информационной безопасности в повестке ООН

Проблема обеспечения международной информационной безопасности была включена в повестку дня ООН по инициативе Российской Федерации уже более 20 лет назад. Впервые она была поставлена в 1998 году в предложении России подписать заявление на уровне президентов РФ и США для создания *международно-правового режима запрещения разработки, производства и применения информационного оружия*. Документ призывал к согласованию на уровне ООН подходов мирового сообщества к применению ИКТ в военных целях, определению терминов «информационное оружие» и «информационная война», анализу возможностей новых технологий для модернизации существующих и создания новых видов вооружений, международному сотрудничеству для мониторинга угроз в информационном пространстве и разработке международного договора о борьбе с терроризмом и преступностью в цифровой сфере. Предложение России не было принято в полном объеме, но проблема была обозначена в подписанном президентами РФ и США по итогам Московского саммита 2 сентября 1998 года «Совместном заявлении об общих вызовах безопасности на рубеже XXI века», в котором признавалась «важность содействия положительным сторонам и ослабления действия отрицательных сторон происходящей сейчас информационно-технологической революции».[3]

23 сентября 1998 года Россия направила специальное Послание по проблеме международной информационной безопасности в адрес Генерального секретаря ООН. К письму прилагался проект резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» для рассмотрения Первым комитетом ГА ООН по вопросам разоружения и международной безопасности. Проект включал предложение для всех государств—членов ООН информировать генерального секретаря о своих взглядах на проблемы МИБ, а также на целесообразность создания международно-правового режима для запрещения разработки опасных видов информационного оружия. Однако в принятой в декабре 1998 года Резолюции A/RES/53/70[4], в отличие от предложенного проекта, не было указания на угрозу применения информационных технологий в военно-политических целях, определений терминов «информационное оружие» и «информационная война» (вместо этого предлагалось определить понятия «несанкционированное вмешательство» и «неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов»), положений о необходимости создания режима запрещения такого оружия, а также о сопоставимости воздействия оружия массового уничтожения (ОМУ) и информационного оружия. Последнее положение могло бы стать основой для использования международного опыта по созданию режимов контроля над ОМУ с целью выработки соответствующего режима для ИКТ-вооружений. По заявлениям российских участников обсуждения, несмотря на критику в адрес первоначального проекта резолюции со стороны представителей США и Великобритании, в заявлении американской делегации отмечалась «гибкость, продемонстрированная основным

[3] Совместное заявление об общих вызовах безопасности на рубеже XXI века. 2 сентября 1998 // Консорциум Кодекс. Электронный фонд правовой и нормативно-технической документации. URL: docs.cntd.ru/document/901764255.

[4] Резолюция, принятая Генеральной Ассамблеей [по докладу Первого комитета (A/53/576)] 53/70. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. 4 января 1999 г. // Организация Объединенных Наций. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R.

спонсором резолюции в продвижении этой инициативы». С тех пор Генеральный секретарь на постоянной основе представляет Генеральной Ассамблее ООН доклад, в котором находят отражение позиции государств по данной проблематике.

Таким образом, инициированная Россией резолюция A/RES/53/70 сыграла основополагающую роль в процессе достижения глобальной цели: обсуждения и создания нового международного режима, т.е. совокупности правил, норм и мероприятий для обеспечения безопасности информации, ИКТ и методов их использования. С 1998 года Россия ежегодно выносит на рассмотрение Генеральной Ассамблеи ООН резолюции под общим названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», соавторами которых становятся все больше государств, что приобрело глобальный характер и охватило уже около 100 стран мира. В течение многих лет резолюции получали одобрение консенсусом. Однако, в 2005–2008 годах проводилось голосование из-за существенных разногласий РФ и США по ряду вопросов, в частности, связанных с понятийным аппаратом и признанием возможности применения ИКТ в военно-политических целях. США стали единственным государством, которое в течение второго президентского срока Дж. Буша-младшего голосовало против этих резолюций. В 2016 году единственной страной, настаивавшей на голосовании, стала Украина, которая в итоге не высказалась «против», а «воздержалась». Голосования в 2018-2019 годах стали результатом начала нового, можно сказать, посткризисного этапа процесса обеспечения МИБ в ООН (таблица 1.1).

Задачи, которые ставились Россией в 1998 году, еще не решены, но с каждым годом обретают все бóльшую актуальность. Поиск ответов сформулированные в ходе обсуждения вопросы привел к созданию *Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ)*, которая стала наиболее важным механизмом Первого комитета ГА ООН в процессе решения проблем информационной безопасности. Первая ГПЭ, в состав которой вошли представители 15 государств, приступила к работе в 2004 году в соответствии с резолюцией ГА ООН A/58/457 [5] и была нацелена на активизацию усилий международного сообщества по исследованию существующих и потенциальных угроз информационной безопасности, возможных ограничительных мер и изучение национальных и международных стратегий безопасности глобальных ИКТ[6].

[5] Резолюция, принятая Генеральной Ассамблеей 8 декабря 2003 года [по Докладу Первого комитета (A/58/457)] 58/32. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485.pdf?OpenElement.

[6] Резолюция, принятая Генеральной Ассамблеей 7 января 2002 года [по Докладу Первого комитета (A/56/533)] 56/19. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement.

Таблица 1.1. Резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», вносимые Россией в 1998–2019 годах

Номер документа	Дата заседания	Результаты голосования
A/RES/53/70	04.12.1998	Приняты без голосования
A/RES/54/49	01.12.1999	
A/RES/55/28	20.11.2000	
A/RES/56/19	29.11.2001	
A/RES/57/53	22.11.2002	
A/RES/58/32	08.12.2003	
A/RES/59/61	03.12.2004	
A/RES/60/45	08.12.2005	**За** – 177, **против** – 1 (США), **воздержались** – 0
A/RES/61/54	06.12.2006	**За** – 176, **против** – 1 (США), **воздержались** – 0
A/RES/62/17	05.12.2007	**За** – 179, **против** – 1 (США), **воздержались** – 0
A/RES/63/37	02.12.2008	**За** – 178, **против** – 1 (США), **воздержались** – 0
A/RES/64/25	02.12.2009	Приняты без голосования.
A/RES/65/41	08.12.2010	
A/RES/66/24	02.12.2011	
A/RES/67/27	03.12.2012	
A/RES/68/243	27.12.2013	
A/RES/69/28	02.12.2014	
A/RES/70/237	23.12.2015	
A/RES/71/28	05.12.2016	**За** – 181, **против** – 0, **воздержались** – 1 (Украина)
A/RES/73/27	05.12.2018	**За** – 119, **против** – 45 (Австралия, Австрия, Албания, Андорра, Бельгия, Болгария, Македония, Венгрия, Германия, Греция, Грузия, Дания, Израиль, Ирландия, Исландия, Испания, Италия, Канада, Кипр, Латвия, Литва, Лихтенштейн, Люксембург, Мальта, Монако, Нидерланды, Новая Зеландия, Норвегия, Польша, Португалия, Румыния, Сан-Марино, Словакия, Словения, Великобритания, США, Украина, Финляндия, Франция, Хорватия, Черногория, Чехия, Швеция, Эстония, Япония, **воздержались** – 14
A/RES/74/29	12.12.2019	**За** – 129, **против** – 6 (Грузия, Израиль, Канада, Великобритания, США, Украина), **воздержались** – 45

Источник: 53-я – 74-я сессии ГА ООН. Резолюции. Первый комитет. Вопросы разоружения и международной безопасности // Организация Объединенных Наций. URL: http://www.un.org/ru/ga/first/53/first_res.shtml ... http://www.un.org/ru/ga/first/70/first_res.shtml ... https://www.un.org/ru/ga/first/74/first_res.shtml.

«Вопросы, связанные с работой группы правительственных экспертов по проблеме информационной безопасности», направленные в Секретариат ООН 28 апреля 2003 года [7], содержали конкретные предложения РФ в контексте деятельности первой ГПЭ. Анализ показывает, что Россия, таким образом, заложила основу для разработки международного, взаимоприемлемого документа, направленного на укрепление МИБ. В соответствии с этими предложениями государства должны нести ответственность за любую осуществляемую ими или с находящихся под их юрисдикцией территорий деятельность в информационном пространстве. Основой будущего режима МИБ могло бы стать обязательство стран-участников об отказе от действий по нанесению вреда критически важной инфраструктуре другого государства, по подрыву политической, экономической и социальной систем, по психологическому воздействию на население для дестабилизации государства и общества. Подготовленный по итогам трех заседаний первой ГПЭ в 2004 году проект доклада не был принят из-за серьезных разногласий, в первую очередь между Россией и США.

В 2005 году «с учетом сложного характера обсуждаемых вопросов не было достигнуто консенсуса относительно подготовки окончательного доклада» [8], был принят лишь процедурный доклад A/60/202. Основные противоречия относились к двум принципиальным вопросам. Первый касался угроз от применения ИКТ в военно-политических целях и негативного воздействия вредоносных информационных технологий на национальную и международную безопасность. На необходимость учета этих угроз, а, следовательно, на важность выработки соответствующего международного документа в рамках Первого комитета ООН, указывали Россия, Белоруссия, Бразилия, КНР, Малайзия, ЮАР и Южная Корея. При этом США, Великобритания, Германия и Франция рассматривали в качестве предмета дискуссии в ООН только криминальную и террористическую составляющие информационной безопасности. Второй вопрос касался необходимости исследования проблем, связанных с содержанием информационных потоков. Россия и ее сторонники полагали, что угрозы, связанные с информационным контентом, должны исследоваться в ГПЭ, а США утверждают, что достаточно учитывать только технические вопросы безопасности информационной инфраструктуры, то есть кибербезопасности в терминологии США. Компромисс по этим двум вопросам до настоящего времени не достигнут.

Однако Группа правительственных экспертов 2-го созыва, созванная в 2009 году по инициативе и под председательством России[9], продолжила обсуждение этих вопросов. Был достигнут некоторый консенсус. На работу Группы в этот период повлияла смена президента США, что привело к признанию со стороны Соединенных Штатов необходимости выработки общей терминологии, а также международных норм и механизмов контроля ИКТ–сферы. В 2010 году после

---

[7] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря. A/58/373. 17 сентября 2003 г. // Организация Объединенных Наций. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/523/42/PDF/N0352342.pdf?OpenElement.

[8] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря. A/60/202. 5 августа 2005 года. // Организация Объединенных Наций. URL: https://digitallibrary.un.org/record/555369?ln=ru.

[9] Резолюция, принятая Генеральной Ассамблеей 6 января 2006 года [по Докладу Первого комитета (A/60/533)] 60/45. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // 15 июля 2011 года. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/490/32/PDF/N0549032.pdf?OpenElement.

четырех сессий ГПЭ выпустила Доклад[10], который позволил впоследствии начать предметную дискуссию по МИБ. Российские предложения поддержали Австралия, Израиль, Канада, Южная Корея и Япония, несмотря на критику американской делегации. В этих предложениях впервые была отмечена угроза целенаправленного создания государствами «ИКТ в качестве инструментов ведения войны и разведки, для применения в политических целях», неопределенность в выявлении источника воздействия, а также риск нестабильности и неправильного восприятия ответных действий государств. Это стало важным фактом признания проблемы применения информационных технологий в военно-политических целях на уровне ООН. Дополнительным доказательством этого стал доклад Генерального секретаря ООН от 15 июля 2011 года A/66/152[11], в который были включены ответы, полученные им от правительств ряда государств, в том США. В ответе США была отмечена проблема «перенесения традиционных форм государственного конфликта в киберпространство», а сами государства включались в число создающих такие угрозы субъектов. В нем также указывалось на то, что «в ряде обстоятельств подрывная деятельность в киберпространстве может представлять собой вооруженное нападение». Однако проблема контента трансграничных информационных потоков до сих пор не рассматривается Соединенными Штатами в плоскости международной информационной безопасности. Деятельность второй ГПЭ по МИБ, по мнению ее российских участников, стала прорывной для России, сумевшей закрепить в повестке ООН наиболее значимые для РФ аспекты. Сегодня можно рассматривать результаты Группы 2009–2010 годов в качестве первых шагов по созданию международного режима контроля над информационным оружием.

Мандат третьей ГПЭ, учрежденной резолюцией ГА ООН A/RES/66/24 от 2 декабря 2011 в составе представителей 15 стран, включал исследование существующих и потенциальных угроз в ИКТ–сфере и возможных стратегий по их минимизации. Доклад Группы, принятый консенсусом всех участников в 2013 году[12], содержал рекомендации по устранению существующих и потенциальных ИКТ–угроз со стороны государств, действующих в их интересах субъектов и негосударственных акторов. При лидирующей роли государства, как указано в документе, гражданское общество и бизнес могут повысить эффективность этого процесса. Таким образом, речь идет о признании принципа ответственности государств за вредоносную деятельность в цифровом пространстве, осуществляемую с их территории, который был предложен Россией в документе, направленном в Секретариат ООН еще в 2003 году. Кроме того, Доклад рекомендовал странам принимать добровольные меры транспарентности и укрепления доверия, расширять международное сотрудничество по обеспечению информационной безопасности не только с развитыми, но и с развивающимися странами. Однако содержащиеся в Докладе 2013 года рекомендации касались лишь увязки вопросов безопасности информационной

[10] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря. A/65/201. 30 июля 2010 года. // http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=/english/&Lang=R.

[11] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад Генерального секретаря. A/66/152. 15 июля 2011 года. // Организация Объединенных Наций. С. 17–25. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/416/93/PDF/N1141693.pdf?OpenElement.

[12] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности Генеральная Ассамблея ООН. A/68/98. 24 июня 2013 года // Организация Объединенных Наций. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/sgreports/68/&Lang=R.

среды с существующими нормами международного права. Достичь компромисса по поставленному Россией вопросу о необходимости принятия дополнительных правовых норм в отношении ИКТ–пространства в тот период не удалось.

ГПЭ 4-го созыва приступила к работе в соответствии с резолюцией ГА ООН A/RES/68/243 от 9 января 2014 года[13] и включала представителей 20 стран. Помимо постоянных задач Группе предстояло продолжить разработку правил ответственного поведения государств в цифровом пространстве, определить условия применения существующих международных норм к ИКТ–среде и выявить случаи необходимости разработки дополнительных норм с учетом уникальных особенностей ИКТ. В начале 2015 года на имя Генерального секретаря ООН было оправлено Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при ООН, в приложении к которому содержались усовершенствованные «Правила поведения государств в информационном пространстве» [14] (первоначальные «Правила поведения» направлялись государствами—членами ШОС в адрес Генерального секретаря ООН в ходе 66-й сессии ГА ООН в 2011 году[15]). В новую редакцию было включено новое правило 3: «Не использовать информационно-коммуникационные технологии и информационные и коммуникационные сети для вмешательства во внутренние дела других государств и в целях подрыва их политической, экономической и социальной стабильности». Было расширено и уточнено правило 7, призывающее «признавать, что права, которые человек имеет в оффлайновой среде, должны также защищаться и в онлайновой среде», возможно, с некоторыми ограничениями в соответствии со ст. 19 Международного пакта о гражданских и политических правах. Дополнительно было разработано правило 10: «Развивать меры укрепления доверия в целях повышения предсказуемости и снижения вероятности недопонимания, а также риска возникновения конфликта. Эти меры включают, среди прочего, добровольный обмен информацией о национальных стратегиях и организационных структурах, направленных на обеспечение информационной безопасности страны, публикацию «белых книг» и обмен наилучшими практиками в тех случаях, когда это практически возможно и целесообразно». Документ закрепляет обязательство государств не применять ИКТ в целях нарушения международной безопасности и для вмешательства во внутренние дела других стран, для дестабилизации их политической, экономической и социальной систем. «Правила поведения» призывают государства воздерживаться от применения силы или угрозы силой в ходе разрешения международных споров в цифровом пространстве.

Итоговый Доклад A/70/174[16] ГПЭ 4-го созыва стал самым содержательным и революционным. Помимо угроз, представленных в предыдущих докладах ГПЭ по

---

[13] Резолюция, принятая Генеральной Ассамблеей 27 декабря 2013 года [по докладу Первого комитета (A/68/406)] 68/243. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. URL: // https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/454/05/PDF/N1345405.pdf?OpenElement.

[14] Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря. A/69/723 // Организация Объединенных Наций. URL: https://undocs.org/ru/A/69/723.

[15] Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря. A/66/359. // Организация Объединенных Наций. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement.

[16] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/70/174/. 22 июля 2015 года // Организация Объединенных Наций. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=R.

МИБ, в разделе II «Существующие и нарождающиеся угрозы» впервые отмечается, что некоторые государства не только наращивают ИКТ–потенциал для применения в военных целях, но и что «использование ИКТ в будущих конфликтах между государствами становится более вероятным». Этого важного дипломатического и политического результата долгое время добивалась Россия. Кроме того, в Докладе впервые речь идет о реальных, а не гипотетических, случаях ИКТ-атак на критически важные объекты государственной инфраструктуры, относящихся «к числу наиболее пагубных нападений с использованием ИКТ». Логично предположить, что такая формулировка, появилась в результате анализа комплексных многоцелевых кибератак на ядерные объекты Ирана в 2010-2012 годов, за которыми с высокой вероятностью стояли государственные структуры. Важное значение в документе уделяется проблеме использования ИКТ террористами, причем не только для вербовки сторонников, финансирования и так далее, но и для совершения нападений на информационные объекты ИКТ и связанную с ними инфраструктуру. Важнейшее положение о необходимости не легализовать и регулировать конфликты в ИКТ–пространстве, как предлагали США и их партнеры, а предотвращать такие конфликты, было поддержано в Докладе 20 странами, поддержавшими применимость международного права к цифровому пространству.

Главным результатом работы ГПЭ 4-го созыва стал пункт 12 итогового Доклада о принятии к сведению «Правил поведения в области обеспечения международной информационной безопасности».

ГПЭ по МИБ 5-го созыва, начавшая свою работу в 2016 году в соответствии с Резолюцией A/RES/70/237 [17] , включала представителей уже 25 стран. Таким образом, с момента созыва первой ГПЭ количество государств—членов Группы выросло с 15 до 25. А число государств, желающих участвовать в ГПЭ, росло в геометрической прогрессии. Важной задачей ГПЭ, по мнению российских представителей, было включение «Правил поведения» в следующую резолюцию Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», что сделало бы «Правила» частью международного «мягкого» права и положило начало формированию системы международных норм в данной области, обеспечению более стабильного миропорядка. Надежда на возможность обсуждения вопросов МИБ на встрече президентов России и Соединенных Штатов в 2017 году и на утверждение «Правил поведения» появилась после прихода к власти президента США Дональда Трампа. Рассматривалась даже возможность подписания двустороннего соглашения о предотвращении инцидентов в информационном пространстве по аналогии с документами, которые касаются инцидентов на море и в воздушном пространстве. Однако, в частности, из-за обвинений России в кибервмешательстве в президентские выборы в США, встреча не состоялась, и надежды на включение «Правил поведения» в следующую резолюцию не оправдались.

2017 год стал кризисным в работе Группы правительственных экспертов по МИБ в ООН. ГПЭ 5-го созыва завершила свою работу 23 июня 2017 года в Нью-Йорке. Предполагалось, что на последнем заседании ГПЭ будет принят итоговой доклад, как это было ранее в 2010, 2013 и 2015 годах. Однако достичь консенсуса не удалось, впервые с 2004 года итоговый документ не был принят. Проект доклада, внесенный немецким председателем на рассмотрение ГПЭ, не был поддержан

[17] Резолюция, принятая Генеральной Ассамблеей 23 декабря 2015 года [по докладу Первого комитета (A/70/455)] 70/237. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. URL: https://undocs.org/ru/A/RES/70/237.

представителями России, стран БРИКС и СНГ, ряда развивающихся государств. Одной из главных, если не основной причиной неудачи стали существенные противоречия между РФ и США по вопросу о праве на самооборону в ответ на кибератаки.

Так, в НАТО было приняло решение о применении Статьи 5 Вашингтонского договора, то есть о возможности реагирования всеми имеющимися средствами, включая военные, в ответ на кибератаку на одного из участников Альянса[18]. А в мае 2019 года партнер США Израиль нанес воздушный удар по зданию на территории Сектора Газа, где, по заявлениям израильских вооруженных сил, готовилось кибернападение с целью нанести урон качеству жизни граждан страны[19]. Таким образом, речь в настоящее время идет уже не о гипотетическом, а о реальном применении военной силы даже не в ответ, а с целью предотвращения кибератак. Россия считает, что источники киберугроз не должны идентифицироваться государствами без доказательств. Некоторые государства, в частности, Куба, полагают, что кибератака не равносильна вооруженному нападению, и поэтому право на самооборону не должно использоваться в таких случаях. Дополнительной «серой зоной» является также право на самооборону от нападений, совершаемых негосударственными субъектами.

В конце 2018 года Первый комитет ООН установил два параллельных процесса обсуждения: в рамках Рабочей группы ООН открытого состава (РГОС) по МИБ[20], и Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ)[21].

С учетом принципов справедливого географического распределения, регионального разнообразия и участия в предыдущих ГПЭ в состав Группы 6-го созыва, образованной по предложению США, вошли 25 стран[22]. Заседания ГПЭ являются закрытыми и не предполагают участия никаких других правительственных или неправительственных наблюдателей. При этом резолюция по ГПЭ предусматривает необходимость проведения консультаций с несколькими региональными организациями[23]. Решения ГПЭ по-прежнему принимаются на основе консенсуса, итоги встреч, как правило, не публикуются, но в конце 2021 года на 76-й сессии ГА ООН может быть представлен итоговый доклад.

Резолюция по РГОС, которая приступила к работе по инициативе России и членом которой могла стать любая страна, предусматривает возможность внесения

---

[18] The North Atlantic Treaty. Washington D.C. 4 April 1949. URL: https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

[19] Doffman Z. Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First // Forbes. 2019. May 6. URL: https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#34426905afb5.

[20] Resolution adopted by the General Assembly on 5 December 2018 [on the report of the First Committee (A/73/505)] 73/27. Developments in the Field of Information and Telecommunications in the Context of International Security // Организация Объединенных Наций. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27.

[21] Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing Responsible State Behavior in Cyberspace in the Context of International Security // Организация Объединенных Наций. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266.

[22] Кения, Маврикий, Марокко, ЮАР; Иордания, Индия, Индонезия, Казахстан, КНР, Сингапур, Япония; Румыния, Россия, Эстония; Бразилия, Мексика, Уругвай; Австралия, Великобритания, Германия, Нидерланды, Норвегия, США, Франция, Швейцария.

[23] ГПЭ предусматривает необходимость проведения консультаций с несколькими региональными организациями, включая Африканский союз (АС), Европейский союз (ЕС), Организацию американских государств (ОАГ), Организацию по безопасности и сотрудничеству в Европе (ОБСЕ) и Ассоциацию государств Юго-Восточной Азии (АСЕАН).

изменений в существующие «Правила поведения» и добавления в них новых пунктов, организации регулярных обсуждений с экспертами из различных областей, а также проблем вредоносного информационного контента.[24] Имея мандат на подготовку консенсусного доклада в конце 2020 года на 75-й ГА ООН по результатам четырех сессий и двух межсессионных консультаций, РГОС обладает уникальными возможностями для поиска точек соприкосновения. В вышедшем в марте 2020 года «Предварительном проекте доклада РГОС о развитии событий в области информации и телекоммуникации в контексте международной безопасности»[25] отмечается, что проблема МИБ охватывает множество областей и дисциплин, а, следовательно, целесообразно использовать результаты обмена мнениями с представителями межправительственных и региональных организаций, НПО, бизнеса и науки. Исходя из анализа ИКТ–угроз международной безопасности и стабильности, РГОС подтвердила растущие тенденции к использованию ИКТ в злонамеренных целях, что может препятствовать получению выгод от таких технологий. Кроме того, в процессе работы Группа признает индивидуальную и общую ответственность государств в цифровой сфере, неравный доступ стран к ИКТ и, следовательно, необходимость уменьшения такого неравенства, а также подчеркивает важность сокращения «гендерного цифрового неравенства» в процессах принятия решений по МИБ.

Обе группы, признавая значение участия бизнеса и научного сообщества и неправительственных организаций (НПО), планируют обсуждение кодекса поведения государств, международных механизмов по борьбе с ИКТ–угрозами и вопросов применения международного права к цифровой среде. Однако новый формат обсуждения проблем МИБ может оказаться еще более сложным, чем ранее. Основные противоречия РФ и США на этом этапе касаются ключевого вопроса: Россия призывает выработать и принять юридически обязывающие правила поведения государств, включив их таким образом в международное право, а США рассматривают существующее право в качестве эффективного и достаточного инструмента для регулирования деятельности в сфере ИКТ. С другой стороны, новый формат может обеспечить и более результативный взаимодополняющий процесс обсуждения. Более того, даже присутствие некоторой конкуренции между ГПЭ и РГОС может мотивировать каждую из групп на достижение более эффективных договоренностей и решений.

Результаты работы ГПЭ и РГОС могут оказать существенное влияние на тенденции и политику в области информационной безопасности в глобальном масштабе. Поэтому научный анализ этих процессов в настоящее время является максимально актуальным.

Одной из главных проблем, по-прежнему, является отсутствие единого международно-правового режима, регулирующего ИКТ–пространство, так как сегодня применяются только некоторые общепринятые нормы международного права и различные внутригосударственные законодательства. При этом необходимо отметить наличие в этих документах противоречий, которые могут быть использованы различными акторами в своих интересах, в том числе вредоносных. В связи с этим основными в обеих группах остаются три направления работы по МИБ:

---

[24] Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Под ред. А.Стрельцова, Э. Тикк, 2020. URL: http://namib.online/wp-content/uploads/2020/07/Brochure_IKT_rus_view.pdf.

[25] Initial “Pre-draft” of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf.

применимость и достаточность международного права; носящие в настоящее время необязательный характер норм поведения стран, так называемые Правила поведения или Кодекс поведения во всемирном цифровом пространстве; меры укрепления доверия между государствами в ИКТ-среде. Новой важной тенденцией, вероятно, станет инициатива по созданию и анализу общих хранилищ данных с позициями государств по вопросам о применении международного права к использованию ИКТ в контексте международной безопасности, а также о практике такого применения. Эту информацию предлагается предоставлять на добровольной основе на веб-портал *Cyber Policy Portal* Института ООН по исследованию проблем разоружения (ЮНИДИР). Логично предположить, что такой подход не должен вызвать серьезных разногласий, так как он нацелен на достижение общего понимания применимости уже согласованных норм и оценку необходимости разработки новых, а также на мотивирование стран к участию в этом процессе. Однако его успех будет зависеть от количества и качества собранной информации и от профессионализма аналитиков. Полезных результатов целесообразно ожидать в случае применения современных максимально объективных количественных методов анализа необходимого и достаточного объема данных.

В этом контексте возникает еще одна ИКТ-проблема, связанная с недостаточной эффективностью методов анализа текстовой информации по сравнению с обработкой структурированной числовой информации. Вид и структура предоставляемых на *Cyber Policy Portal* ЮНИДИР данных должны быть унифицированы и глубоко продуманы. А сами эти данные должны максимально исключать политизацию процесса. Однако это вряд ли полностью достижимо. Поэтому для получения объективных результатов необходима высокопроизводительная аналитика нового уровня, включающая в анализ неструктурированную текстовую информацию. Возможность извлечения полезных сведений из предоставленной неструктурированной текстовой информации станет ключевой задачей в этом новом процессе ООН.

Дополнительным инструментом текстовой аналитики может стать научный анализ по сопоставлению и сравнению предоставленных в ЮНИДИР данных с той информацией о прецедентах применения правовых норм к ИКТ-пространству, которые обсуждаются на международных и внутригосударственных конференциях, на мероприятиях институтов и организаций. Это позволит выявить реальные опасения и насущные вопросы, которые могут не озвучиваться в официально предоставляемых в ООН сведениях. Тогда так называемая, обратная связь от государств даст возможность сделать полезные выводы, которые впоследствии должны стать частью повестки дня групп ООН по соответствующему направлению.

В настоящее время методы, позволяющие решить такие задачи, активно развиваются на базе машинного обучения и искусственного интеллекта. Это технологии получения информации из неструктурированного исходного текста путём их преобразования в набор структурированных данных в удобном для компьютера формате. Как правило, такие методы включают синтаксический и лингвистический анализ, категоризацию, кластеризацию, извлечение концептов (сущностей), моделирование отношений между сущностями, тематическое индексирование, контент-анализ, изучение частотных распределений слов, аннотирование и т.д. Интерпретация результатов также происходит с помощью методов интеллектуального анализа данных. Подобные ИКТ сегодня уже широко применяется в бизнесе, науке, государственном управлении, системах безопасности и разведки. Таким образом, если современные кибертехнологии будут применяться непосредственно в области обеспечения международной информационной

безопасности в ООН, это станет лучшим доказательством поддержки современных мирных ИКТ в противовес противодействию их вредоносному использованию.

Негативное влияние на достижение компромисса между государствами и группами ООН продолжают оказывать разногласия относительно целесообразности разработки специальных международно-правовых норм, применимых в случае использования ИКТ в военных целях. Рассматривая проблему как неактуальную на данном этапе, США считают, что сначала необходимо накопить достаточный практический опыт урегулирования инцидентов. Россия же по-прежнему убеждена, что основной целью должно стать предотвращение применения ИКТ в военно-политических целях.

Серьезных усилий дипломатии в рамках работы обеих групп потребуют следующие вопросы:

- применимость международного права к ИКТ–атакам в мирное время;
- контроль над распространением информационного оружия;
- контроль над ИКТ двойного назначения;
- применимость Устава ООН к киберпространству, в частности, право на самооборону;
- превентивные меры предотвращения ИКТ–атак, в частности, вопрос об уведомлении перед применением контрмер;
- атрибуция ИКТ–атак;
- использование ИКТ для нарушения суверенитета и вмешательства во внутренние дела государств;
- обязательство государств не допускать использования их территории для совершения ИКТ–атак государственными или негосударственными субъектами против других государств;
- инструменты координации ответственного поведения государств в ИКТ–пространстве;
- принцип обязательности “Правил поведения”, возможность их расширения;
- роль ООН в разработке мер доверия;
- базовые права человека в процессе применения новых норм и правил поведения в ИКТ–пространстве;
- наращивание потенциала информационной безопасности;
- выработка единого понятийного аппарата по МИБ;
- оценка равной применимости «Правил поведения» в военное и мирное время;
- функции и координация работы ГПЭ и РГОС.

В ходе анализа и прогнозирования перспектив МИБ необходимо учитывать важнейшие политические характеристики современного этапа, не способствующие эффективности процесса. Они связаны с недостаточным сотрудничеством «великих держав» в этой области, с отсутствием прозрачности в отношениях между государствами, что затрудняет оценку приверженности стран нормам и принципам поведения в цифровом пространстве. Недостаточно четкие стимулы для выполнения норм и отсутствие конкретных выгод от этого существенно тормозят разработку международного режима управления и контроля над вредоносными ИКТ. Таким образом, расширение исследований по оценке существующих правил, применимых к информационному пространству, а также по выявлению дополнительных норм является в настоящее время максимально актуальным. Параллельно целесообразно вести работу по классификации угроз в данной сфере на международном уровне, а также по мониторингу опасных инцидентов с

применением ИКТ. Междисциплинарный и мультидисциплинарный анализ существующих угроз МИБ, научное прогнозирование и планирование будущих опасностей со стороны научно-экспертного сообщества приобретает, таким образом, еще более важное значение.

1.3. Военно-политические проблемы международной информационной безопасности

Одна из важнейших актуальных тенденций связана с тем, что для большинства стран мира стратегическое значение имеет защищенность ИКТ-систем, которые стали важным фактором обеспечения суверенитета, обороноспособности и безопасности государства. При этом речь сегодня идет об угрозе ускоренного развития (гонки) информационных вооружений. По некоторым оценкам, уже более 30 государств обладают наступательным кибернетическим оружием (кибероружием).[26] ИКТ могут спровоцировать развязывание межгосударственного военного конфликта, в первую очередь, из-за возможности несоразмерного использования методов реагирования на угрозы и атаки: пострадавшая сторона может применить в ответ реальное оружие. Кроме того, конфликт может возникнуть по ошибке, т.к. в настоящее время отсутствует универсальная методология идентификации нарушителей, не выработаны критерии отнесения кибератак к вооруженному нападению, не сформированы универсальные принципы расследования инцидентов.

Еще одной глобальной проблемой является информационная безопасность военных объектов как части критически важной инфраструктуры (КИ), к которой относят системы и средства, которые настолько жизненно важны для страны, что нарушение их работы или уничтожение окажет необратимое негативное воздействие на национальную и экономическую безопасность, здравоохранение, правопорядок и т.д. (рисунок 1.1). Под ***безопасностью КИ*** в этом контексте понимается *защищенность от угроз, реализуемых посредством применения специальных информационных технологий для разрушения либо для недопустимого использования этих объектов*. Даже если эти объекты не подключены к Интернету напрямую, устройства автоматизированной системы управления технологическим процессом (АСУ ТП), используемые для дистанционного контроля по защищенным коммуникационным линиям, могут быть взломаны в результате атаки на другие объекты, на которых функционируют АСУ ТП. Изоляция сети от внешних систем, считавшаяся незыблемым требованием 10–15 лет назад, больше не рассматривается как эффективная защитная мера, т.к. стала невыгодной экономически и трудно реализуемой на практике. Поэтому угроза крупномасштабной комплексной атаки на КИ более чем реальна и быстро возрастает. При этом необходимо учитывать тесную взаимосвязь гражданских обеспечивающих систем КИ с военной инфраструктурой.

Сегодня уже десятки стран обладают программным обеспечением (ПО) для нападения на объекты КИ. При этом показатель опасности для АСУ ТП в настоящее время оценивается специалистами как критический или высокий. В 2019 году были зафиксированы ежемесячные кибератаки на каждый четвертый компьютер на промышленных предприятиях России. Вредоносные программы разрабатываются в настоящее время во многих странах, однако 83% всех площадок, используемых для

[26] Ромашкина Н.П. Стратегическая стабильность: новые вызовы инфосферы // Российский совет по международным делам. 2017. 23 ноября // http://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-stabilnost-novye-vyzovy-infosfery/.

распространения «зловредов», расположены всего в 10 государствах. Лидером этого рейтинга являются США, где находится четверть всех источников заражения.

Целями таких «вредоносов» могут быть органы государственной власти, банки, спутниковые, нефтегазовые и транспортные системы, электро- и атомные станции, коммуникационные системы, порты, аэропорты, военные объекты, что грозит страшными последствиями как на государственном, так и на глобальном уровне. Таким образом, подобные вредоносные программы представляют собой перспективное стратегическое оружие, а растущая сложность оборудования и программного обеспечения объектов критической инфраструктуры ведет к росту вероятности ошибок и уязвимостей, что может быть использовано противником.

К общемировым тенденциям, увеличивающим угрозы для таких объектов относятся использование личных мобильных устройств на объектах КИ; переход на цифровые системы управления производственными и технологическими процессами; подключение офисных и промышленных корпоративных сетей к Интернету; сложность трансконтинентальных цепочек поставок программного обеспечения систем управления производственными и технологическими процессами. Эти тенденции касаются всех объектов КИ. Но наибольшее беспокойство вызывают угрозы автоматизированным системам боевого управления (АСБУ) ядерным оружием (ЯО) – связи, командования и контроля над ЯО (С3) в западной терминологии. Угрозы, создающие проблему обеспечения ИКТ-безопасности объектов военно-промышленного комплекса (ВПК), признаки наличия и возможности осуществления этих угроз представлены в таблице 1.2.

Рисунок 1.1. География атак* на системы промышленной автоматизации, второе полугодие 2019 года

* процент компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Источник: «Лаборатория Касперского», https://ics-cert.kaspersky.ru/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-overall-global-statistics-h2-2019.

Таблица 1.2. Проблема обеспечения информационной безопасности военных объектов как части критически важной инфраструктуры государства

Угроза	Признаки наличия угрозы	Возможности осуществления угрозы
Развитие ИКТ-средств для вредоносного воздействия на объекты ВПК	Наличие ИКТ-угроз для различных элементов военной организации и инфраструктуры. Важнейшие: стратегические вооружения, система предупреждения о ракетном нападении (СПРН), система командования и контроля над ядерным оружием (ЯО), ПРО, ПВО.	• Кибернападения на объекты военной или связанной с ней гражданской инфраструктуры; • физический вред ПО, элементной базе, линиям связи и сетям военного объекта; • дистанционный «логический» вред с помощью вредоносных программ, «логических бомб» и т.д.; • умышленный или непреднамеренный удаленный вред через компьютерные сети (в т.ч. Интернет) или в результате контакта с компьютером; • кибершпионаж и создание киберагентурных сетей; • киберсаботаж; • создание неуверенности командования и персонала в бесперебойной и эффективной работе систем.
	Рост масштабов применения ударных роботизированных средств с дистанционным управлением, искусственного интеллекта в военных целях, автоматизированных систем (АС) принятия решений и т.д., которые могут подвергаться кибератакам.	
	Перевод войск стратегического назначения в разных странах на цифровые технологии передачи информации, что сделает их более уязвимыми для технических ошибок и преднамеренных кибератак.	
Снижение уровня стратегической стабильности	Влияние развития ИКТ на рост вероятности:	
	• ошибочного санкционированного пуска баллистических ракет (БР);	
	• получения ложной информации от СПРН о запуске БР со стороны противника из-за растущей изощренности кибератак;	
	• повреждения или разрушения каналов коммуникаций, создания помех в системе управления вооруженными, в том числе, ядерными, силами;	
	• снижения уверенности военных, принимающих решения, в работоспособности систем управления, командования и контроля ВС.	
	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.	

Источник: таблица построена автором.

1.4. Вызовы для России в сфере информационной безопасности

Анализ глобальных ИКТ-угроз международному миру и безопасности приводит к выводу о целесообразности создания системы сдерживания применения информационного оружия, и, как следствие – глобальной информационной войны. Исходя из того, что методы с использованием современных ИКТ превращаются в важный элемент военного потенциала государств, дополняющий обычные военные средства, а новые технологии могут стать детонатором развязывания межгосударственного военного конфликта, одной из важнейших задач государства в процессе построения системы, основанной на концепции сдерживания, становится совершенствование законодательного и технологического обеспечения национальной информационной безопасности.

Для России одной из важнейших задач в этой области является сегодня создание необходимой законодательной базы. Ее решение должно включать:

1) сбор и анализ информации о состоянии и проблемах российского законодательства, регулирующего вопросы безопасности, развития и использования цифровых технологий;
2) мониторинг законодательства России и иностранных государств, регулирующих вопросы информационной безопасности, который должен вестись на постоянной основе экспертами инициативно и по запросу парламента;
3) совершенствование российского законодательства, регулирующего вопросы развития и использования цифровых технологий, информационно-психологической и информационно-технологической безопасности, что приведет к постоянному совершенствованию государственной политики в этой сфере.

В рамках научного подхода к проблеме законодательного обеспечения информационной безопасности можно выделить следующие признаки наличия проблемы.

1. *Несогласованность между современными ИКТ (большие данные, облачные технологии, суперкомпьютеры, искусственный интеллект и т.д.) и российским законодательством,* регулирующим вопросы безопасности в информационной сфере, развития и использования цифровых технологий. Например, несмотря на лавинообразный рост возможностей для сбора в Интернете личных данных граждан (персональные данные являются их частью) и использования их массивов (так называемых, «больших данных»), до сих пор эта сфера не упорядочена и не введена в правовое поле. При этом массивы могут использоваться во вредоносных, в том числе военно-политических целях. Кроме того, эти данные накапливаются и могут быть использованы против человека спустя много лет. Таким образом, законодательное регулирование таких процессов является частью информационной безопасности государства.

2. *Дороговизна и сложность технической защиты информационных систем персональных данных.*

3. *Неоднозначность некоторых положений законов*, которые по-разному трактуются государственными регуляторами и операторами и требуют конкретизации, уточнений и разъяснений. Кроме того, существует проблема терминологии. В ООН по инициативе России используется компромиссный термин «информационно-коммуникационные технологии», ИКТ. В официальных документах РФ также отсутствует термин «кибер», «кибернетический», «кибербезопасность» и т.д. Но при этом в технических регламентах и ГОСТах термин «кибер» активно используется.

4. *Зависимость информационной безопасности РФ от иностранных поставщиков* программно-аппаратных компонентов ПО и оборудования. Так, большинство интернет-технологий (браузеры, поисковики, социальные сети, операционные системы и др.) находится вне пределов российского контроля. Это создает дополнительные угрозы безопасности. Поэтому государству следует иметь полную технологическую цепочку, начиная от процессора и заканчивая конечным ПО.

5. *Уязвимость элементов информационной безопасности* в связи с нехваткой квалифицированных специалистов, программного обеспечения и недостаточной координации с правоохранительными органами. Необходимость использования системы всемирных межбанковских финансовых каналов связи (Society for Worldwide Interbank Financial Telecommunications (SWIFT)) для международных расчетов.

6. *Опережение развития атакующих ИКТ-технологий по сравнению с защитными у лидеров ИКТ-индустрии* (в частности, в отношении сведений, содержащих государственную или коммерческую тайну, а также серверов государственных учреждений и других объектов критически важной государственной инфраструктуры), что требует постоянного мониторинга законодательства РФ и иностранных государств, регулирующих вопросы информационной безопасности.

7. *Рост рисков ущерба репутации государства в связи с вредоносным использованием ИКТ в условиях политической конкуренции*, что может выражаться не только в репутационных, но и в финансовых потерях.

8. *Необходимость адаптации российского законодательства к глобальным угрозам информационной безопасности* (в частности, разработка и принятие Стратегии информационной безопасности РФ).

9. *Необходимость совершенствования законодательства РФ,* способствующего созданию международной нормативно-правовой базы по борьбе с ИКТ-угрозами.

10. *Целесообразность гармонизации и унификации законодательств государств - союзников и партнеров РФ* в сфере информационной безопасности в условиях формирования глобального информационного пространства и ускоренного роста глобальных угроз информационной безопасности.

На современном этапе одним их основных стратегических приоритетов государственной политики стало повышение значимости обеспечения информационной безопасности в качестве системообразующего элемента управления, а также совершенствование нормативно-правового обеспечения в ИКТ-сфере. В настоящее время законодательство РФ в сфере ИКТ переживает стадию роста и отвечает не всем требованиям, позволяющим обеспечить информационную безопасность в полном объеме. Таким образом, ***целью*** является *создание механизма, позволяющего согласовать процесс разработки законов с существующими реалиями и прогрессом ИКТ для обеспечения информационной безопасности государства*.

Основные ***задачи*** для достижения этой цели связаны с качеством государственного управления и уровнем информационной безопасности, которые в целом определяются способностью государства:

1) обеспечить функционирование информационных ресурсов и потоков, необходимое и достаточное для устойчивой жизнедеятельности и развития;
   противостоять техническим и психологическим угрозам;
2) защитить в полном объеме государственную и коммерческую тайну от незаконных посягательств;

3) поддерживать эффективность работы, возможность «саморазвития» и адекватные реакции системы на возрастающие вызовы;
4) обеспечить устойчивость и безопасность государства от ИКТ-угроз в военно-политической сфере.

Первостепенными задачами экспертного сообщества при этом являются:

1) подготовка предложений и рекомендаций, включающих в себя результаты исследований с применением традиционных и современных междисциплинарных методов для выявления внутрисистемных и межсистемных противоречий, социально-правовых и политических проблем в сфере ИКТ;
2) разработка *методологии* выявления правовых проблем в ИКТ-сфере, а также общих социально-политических условий подготовки и принятия законодательных актов для постоянного совершенствования законодательства в сфере информационных технологий.

Таким образом, результатом деятельности экспертов из разных областей должно стать создание постоянно действующего механизма, который позволит согласовать процесс разработки законов с существующими реалиями и прогрессом ИКТ для обеспечения информационной безопасности государства. В обозримой перспективе этот механизм целесообразно настроить на применение *комплексного подхода*:

1) внесение изменений в существующее законодательство, исходя из анализа практики применения и новых условий, связанных с ускоренным развитием ИКТ;
2) параллельная работа по подготовке Стратегии информационной безопасности РФ;
3) подготовка новых нормативно-правовых актов после выхода Стратегии информационной безопасности РФ.

Целесообразность создания системы сдерживания вредоносных ИКТ на данном этапе подтверждается постоянным совершенствованием нормативно-правовой базы в государствах с наиболее развитыми ИКТ, которая является основой их политики в информационном пространстве. Так, в сентябре 2018 года в США была утверждена новая Национальная киберстратегия (*National Cyber Strategy of the United States of America)*[27]. Предыдущая киберстратегия была принята в США 15 лет назад. Анализ структуры документа, представленной в таблице 1.3, позволяет сделать выводы о тщательности его подготовки.

Не вдаваясь в детальный анализ новой киберстратегии США, полезно напомнить лишь некоторые ее положения:

1. «В настоящей стратегии излагаются методы, с помощью которых моя администрация будет: обеспечивать безопасность Америки путем защиты сетей, систем, программных функций и данных; обеспечивать процветание Америки путем построения безопасной, успешной цифровой экономики и стимулирования развития инноваций на национальном уровне; обеспечивать мир и безопасность путем увеличения возможностей США совместно с их союзниками и партнерами по сдерживанию, а, при необходимости, и по наказанию лиц и государств, использующих цифровые инструменты в злонамеренных целях; расширять американское влияние за рубежом с целью более широкого внедрения основных принципов открытого, функционально совместимого, надежного и безопасного интернета».

[27] National Cyber Strategy of the United States of America. September 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

2. «Россия, Китай, Иран и Северная Корея используют киберпространство в качестве площадки, где они могут бросить вызов Соединенным Штатам, нашим союзникам и партнерам… Россия, Иран и Северная Корея провели ряд хакерских атак, которые нанесли ощутимый ущерб американским и транснациональным компаниям, нашим союзникам и партнерам и не понесли соответственного наказания, что могло бы стать сдерживающим фактором от осуществления подобных хакерских атак в будущем. Китай использует киберпространство для осуществления экономического шпионажа и кражи объектов интеллектуальной собственности, стоимость которой измеряется триллионами долларов».
3. «Нынешняя администрация уже приняла ряд мер по активному устранению этих угроз и адаптации к новым реалиям. Мы наложили на опасных внешних злоумышленников соответствующие санкции. Мы поименно назвали наших противников, осуществлявших подрывную деятельность, и опубликовали информацию о совершенных действиях, а также используемых ими инструментах и методах. Мы обязали государственные органы и ведомства заменить программное обеспечение, имеющее критические уязвимости для обеспечения безопасности».
4. «Соединенные Штаты намерены сотрудничать с государствами-единомышленниками по вопросам координации и оказания поддержки применения мер реагирования друг друга в отношении серьезных злоумышленных инцидентов в киберпространстве, в том числе посредством обмена разведывательными данными, подкрепленными источниками, публичными заявлениями о поддержке мер реагирования, а также совместным применением мер реагирования против злоумышленников».
5. «Наши конкуренты реализуют программы подготовки трудовых ресурсов, которые могут нанести вред конкурентоспособности Соединенных Штатов в сфере кибербезопасности в долгосрочной перспективе. Правительство Соединенных Штатов продолжит финансировать и расширять программы, которые создают качественный национальный кадровый резерв, как в начальной школе, так и в рамках высших учебных заведений. Нынешняя администрация будет внедрять предложенные Президентом иммиграционные реформы, основанные на заслугах кандидатов, с целью создания в Соединенных Штатах наиболее конкурентоспособного технологического сектора».

Таблица 1.3.
Структура Национальной Киберстратегии США (National Cyber Strategy of the United States of America)

Название	Содержание
Введение	*Анализ текущей ситуации* *Стратегия развития*
I **Защита американского народа, Америки и американского образа жизни**	***Безопасность федеральных сетей и информации*** *Дальнейшая централизация управления и контроля в сфере федеральной гражданской кибербезопасности* *Согласование деятельности в области управления рисками и информационных технологий* *Совершенствование управления рисками в федеральной системе поставок* *Укрепление кибербезопасности федеральной контрактной системы* *Обеспечение лидирующей роли правительства в области передовой и инновационной практики*
	Безопасность критически важной инфраструктуры *Уточнение ролей и обязанностей* *Приоритетность действий в соответствии с выявленными национальными рисками* *Использование поставщиков ИКТ в качестве средств обеспечения кибербезопасности* *Защита нашей демократии* *Стимулирование инвестиций в кибербезопасность* *Приоритетность инвестиций в национальные исследования и разработки* *Совершенствование транспортной и морской кибербезопасности* *Совершенствование Космической Кибербезопасности*
	Борьба с киберпреступностью и совершенствование отчетности об инцидентах *Совершенствование отчетности об инцидентах и реагировании на них* *Модернизация законов об электронном наблюдении и компьютерной преступности* *Снижение угроз со стороны транснациональных преступных организаций в киберпространстве* *Совершенствование системы задержания преступников заграницей* *Усиление правоохранительного потенциала стран-партнеров для борьбы с киберпреступностью*

Название	Содержание
II **Обеспечение процветания Америки**	***Содействие динамичной и устойчивой цифровой экономики*** *Стимулирование развития рынка адаптивных и безопасных технологий* *Приоритеты инновационной деятельности* *Инвестиции в инфраструктуру следующего поколения* *Содействие свободному трансграничному потоку данных* *Сохранение лидерства США в передовых технологиях* *Продвижение кибербезопасности с полным жизненным циклом*
	Содействие развитию и защита изобретений в США *Совершенствование механизмов анализа иностранной инвестиционной деятельности в США* *Поддержание сильной и сбалансированной системы защиты интеллектуальной собственности* *Защита конфиденциальности и целостности американских идей*
	Развитие исключительных человеческих ресурсов, обеспечивающих кибербезопасность *Создание и поддержание конвейера талантов* *Расширение возможностей переквалификации и образования для американских рабочих* *Повышение уровня федеральных специалистов по кибербезопасности* *Использование исполнительной власти для выявления и поощрения талантов*
III **Сохранение мира силовыми методами**	***Повышение киберстабильности через нормы ответственного поведения государств*** *Поощрение всеобщего соблюдения кибернорм*
	Атрибуция и сдерживание неприемлемого поведения в киберпространстве *Целевое лидерство и совместная разведка* *Применение мер реагирования* *Создание инициативы кибersдерживания* *Противодействие вредоносному кибервоздействию и информационные операции*
IV **Продвижение американского влияния**	***Продвижение открытого, интероперабельного, надежного и безопасного Интернета*** *Защита и продвижение свободы Интернета* *Работа со странами-единомышленниками, промышленностью, научными кругами и гражданским обществом* *Продвижение многосторонней модели управления Интернетом* *Продвижение совместимой и надежной инфраструктуры связи и доступа к Интернету* *Продвижение и сохранение международных рынков для изобретений США*
	Создание международного киберпотенциала *Расширение возможностей по наращиванию киберпотенциала.*

Источник: National Cyber Strategy of the United States of America, September 2018.

Кроме Национальной Киберстратегии в США действует *Киберстратегия Министерства обороны США*, а также *Стратегия Объединенного киберкомандования Вооруженных сил США* (функциональная структура, объединяющая более 6000 специалистов из разных военных ведомств и командований) под названием «Завоевание и удержание господства в киберпространстве»[28]. Важное значение в этом контексте имеет также решение НАТО о возможности задействовать статью 5 Вашингтонского договора, предусматривающую коллективную самооборону, в случае кибернападения, хотя при этом подчеркивается, что не любое кибернападение приведет к задействованию статьи 5[29]. Следовательно, в США существует комплексная стратегическая программа обеспечения и поддержания информационного превосходства путем повышения своих возможностей и всестороннего снижения способностей других акторов. Таким образом, речь сегодня идет уже не о предпосылках возникновения новой сферы соперничества в информационном пространстве, а о том, что новая эра стратегического противоборства – ИКТ-противоборства – с указанием лидера в лице США, противников, среди которых названа Россия, детального пошагового системного плана действий, а также конкретных мер противодействия и «наказания» противников – уже наступила (рисунок 1.2).

Рисунок 1.2. Государства–партнеры РФ и США в области информационной безопасности

Источник: рисунок построен автором.

[28] Department of Defense Cyber Strategy 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_

[29] НАТО готова к коллективной обороне при кибератаках, но не во всех случаях. // РИА Новости. 2016. 14 июня. URL: http://ria.ru/world/20160614/1447513284.html#ixzz4Be5c0CYs.

В таких условиях обеспечение безопасной ИКТ-среды как части системы глобальной международной безопасности требует от России принятия специальных мер. В частности, целесообразно ставить вопрос о необходимости разработки российской Стратегии информационной безопасности. Это обосновано также тем, что стратегические документы, на юридической основе определяющие направления и перспективы развития государства (а ИКТ являются одной из важнейших характеристик развития) играют особую роль на современном этапе и создают правовой фундамент инновационного развития, определяя основы государственной политики.

Важнейшими характеристиками стратегии в отличие от всех других видов документов, в частности, являются:

1) целевой подход к разработке, основанный на определении важнейшей цели и задач по ее достижению, приоритетность которых определяет содержание и сущностные результаты действий по развитию соответствующей сферы;

2) системный подход к реализации, предусматривающий решение указанных задач и, соответственно, максимальный охват всех основных направлений, которые должны быть задействованы в реализации стратегических установок государственной политики в соответствующей области;

3) комплекс конкретных согласованных и взаимосвязанных мероприятий, средств и ресурсов, обеспечивающих достижение результатов, предусмотренных указанными задачами в рамках каждого из приоритетных направлений;

4) действия по единому поэтапному плану с четко обозначенными целевыми индикаторами и показателями на каждом из этапов, а также разработанной системой финансирования основных мероприятий;

5) мониторинг за ходом реализации стратегии и применение системы мер юридического контроля за достижением конечных и промежуточных результатов.

Таким образом, стратегия разрабатывается в рамках *определения цели и постановки задач, прогнозирования, планирования и программирования* на федеральном уровне, на уровне субъектов Российской Федерации и на уровне муниципальных образований. Очевидно, что ***Стратегия*** *как система формально-определенных положений, закрепляющих стратегическую цель, задачи и направления деятельности органов государственной власти по ее достижению, средства и ресурсы, которые могут быть на это затрачены*, существенно отличается от ***Доктрины*** (в России действует Доктрина информационной безопасности [30]), *которая по сути представляет собой философскую, политическую либо правовую теорию, концепцию, учение, систему воззрений, руководящий теоретический или политический принцип*.

Стратегия информационной безопасности России должна стать фундаментом развития информационной сферы в стране, обеспечивающим организационные, законодательные и экономические условия и гарантии безопасного эволюционного процесса. Документ призван сформулировать цель и задачи развития, а также защиты от угроз и рисков в информационном пространстве. Стратегия должна описывать комплексный системный подход к реализации указанных цели и задач, согласованные и взаимосвязанные действия и мероприятия, которые базировались бы на целевых индикаторах и показателях на каждом этапе реализации. Важной частью стратегии является также четко прописанная система мониторинга и мер юридического контроля за достижением конечных и промежуточных результатов. Такой документ может сыграть важную роль в формировании режима контроля над ИКТ-вооружениями.

---

[30] Доктрина информационной безопасности Российской Федерации. Гарант.ру // https://www.garant.ru/products/ipo/prime/doc/71456224/.

ГЛАВА 2.

Программные системы и международная информационная безопасность

2.1. Проблематика безопасности программных систем

Одной из важнейших тем международной информационной безопасности является свод из тринадцати международных правил, норм и принципов ответственного поведения государств, рекомендованный Резолюцией Генеральной Ассамблеи ООН A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [31]. Подчеркивая значимость этих правил, следует отметить, что основное внимание в них обращено на конкретные действия мирового сообщества в рамках жизненного цикла международных конфликтов в сфере ИКТ (в том числе в информационном и киберпространствах[32]), а именно в латентной и открытой фазах киберконфликта. Важность таких обсуждений, в частности, подтверждена использованием Израилем летального оружия в Секторе Газа в ответ на готовящиеся враждебные целенаправленные компьютерные атаки со стороны движения ХАМАС [33].

Вместе с тем объективные причины возникновения киберконфликта, связанные с правовым и специальным (техническим) регулированием безопасности компьютерных систем, исследованы в настоящее время весьма скупо. В первую очередь это касается программных систем, которые являются системообразующим элементом сферы ИКТ, ее продуктом и одним из главных источников нестабильности. Рассматривая жизненный цикл программных систем и их роль в процессе обеспечения МИБ, следует специально подчеркнуть пункты 9 и 11 указанного свода правил, норм и принципов, а именно:

- государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ;
- государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры.

Данная глава посвящена обоснованию целесообразности уточнения и изменения указанных пунктов в части исследования объективных факторов возникновения, эксплуатации и устранения уязвимостей программ, а также связанных с ними угроз и рисков в контексте международной безопасности.

Следует добавить, что вопросы транспарентности действий мирового сообщества в сфере ИКТ, исключительной предпочтительности предупредительных

---

[31] Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года [по докладу Первого комитета (A/73/505)] 73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций. URL: https://undocs.org/ru/A/RES/73/27.

[32] В главе наряду с терминологической базой сферы ИКТ для обеспечения полноты исследования используются устоявшиеся определения в области кибербезопасности, принятые международными сообществами, в которых участвует Россия, таких как ИСО (ISO), МЭК (IEC) и МСЭ (ITU).

[33] Israel Defense Forces. Official IDF Twitter. URL: https://twitter.com/idf/status/1125066395010699264.

механизмов МИБ[34], а также повышения доверия (путем правового и технического регулирования) к безопасности программных систем в контексте международной безопасности являются максимально актуальными и востребованными.

2.1.1. Терминологический аппарат безопасности программ

В общем плане *под **международной информационной безопасностью** понимают состояние (свойство) защищенности глобального информационного пространства от угроз информационной сферы*. К сожалению, по политическим соображениям угрозы информационной сферы разными странами трактуются по-разному, что исключает точное определение.

В отношении разграничения информационных активов и соответствующих им угроз технического характера выделяют понятие ***информационной безопасности компьютерных систем*** (как состояние защищенности активов от угроз целостности, доступности и конфиденциальности) и далее ее подсвойство – ***безопасность программных систем***.

Под ***кибербезопасностью*** понимают *свойство защищенности активов киберпространства*, однако в настоящее время также налицо различная трактовка степени виртуальности (то есть, границы) киберпространства и учитываемый класс угроз (целенаправленного, военного или любого характера). Например, различные интерпретации киберпространства представлены во многих документах национальных и международных организаций и сообществ, таких как Министерство обороны США, МСЭ (ITU), ИСО (ISO) и другие.

При исследовании безопасности программных систем в первую очередь выделяют понятие ***безопасного программного обеспечения***, под которым понимают *программное обеспечение (ПО), создаваемое с применением мер безопасности, направленных на исключение уязвимостей при разработке и внедрении, а также своевременное их устранение в случае обнаружения в процессе жизненного цикла систем*. Опираясь на теорию информационной безопасности, следует выделить факторы безопасности программного обеспечения на этапах его следует выделить факторы безопасности программного обеспечения на этапах его жизненного цикла, а именно: дефект, уязвимость, угроза и риск (рисунок 2.1).

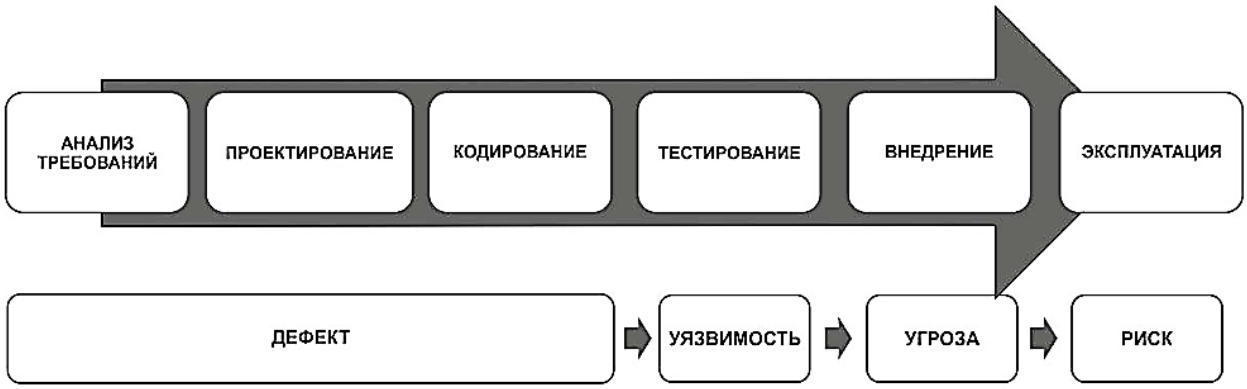
Дефект (недостаток, некорректность, weakness) – это *любая ошибка, допущенная в ходе проектирования или реализации программы, которая, в случае ее неисправления, может являться причиной уязвимости программы (то есть потенциально повлиять на уровень информационной безопасности системы)*.

Уязвимость (vulnerability) – *недостаток программы, который может быть использован для реализации угроз безопасности информации*. Наличие уязвимости может составлять ***угрозу информационному ресурсу (или активу)***, если ее можно реализовать с целью снижения уровня информационной безопасности системы.

Комбинация (как правило, умножение) величины возможного ущерба и вероятности реализации угрозы составляет ***риск информационной безопасности систем***.

[34] Шерстюк В.П. Меры доверия должны расширять, повышать. Только тогда можно будет достичь чего-то // Международная жизнь. 2019. 25 апреля. URL: https://interaffairs.ru/news/show/22336.

Рисунок 2.1. Факторы программной безопасности



Источник: рисунок построен автором.

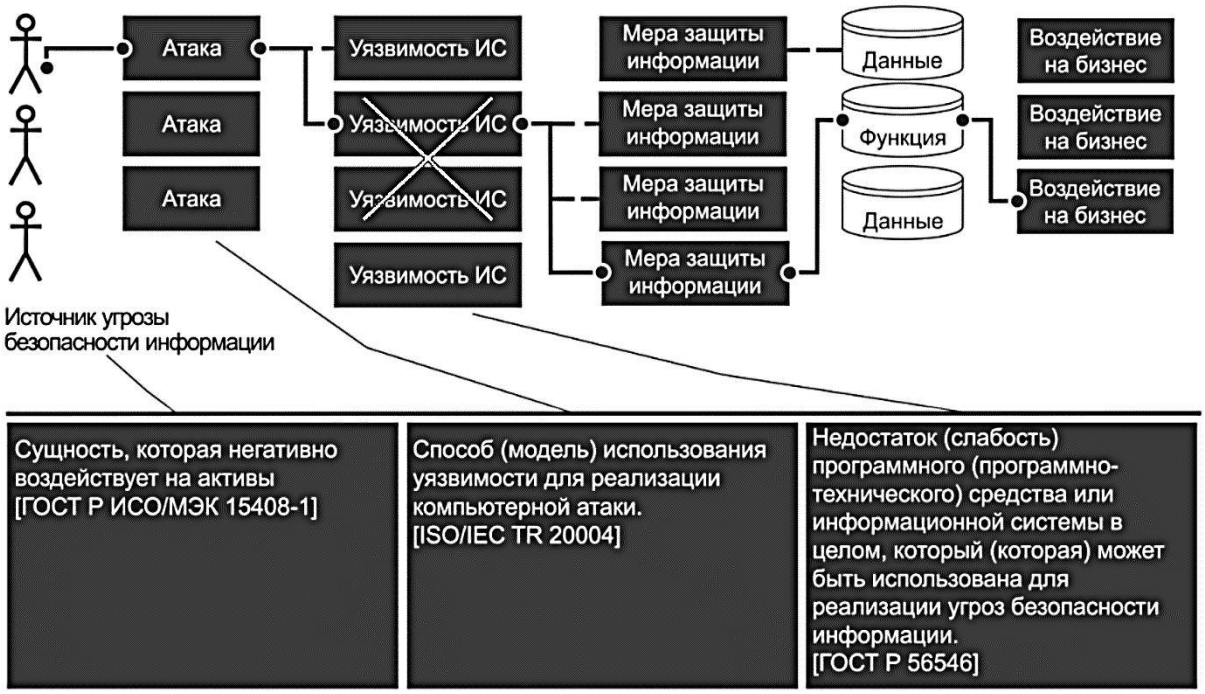
Можно утверждать, что в настоящее время понятийная база программной безопасности сложилась и находится на соответствующем уровне итерационного развития современной парадигмы информационной безопасности. Этому свидетельствуют современные систематики дефектов, уязвимостей и атак (например, рисунок 2.2).

Рисунок 2.2. Фрагмент онтологии MITRE с примерами для исследователей

Источник: MITRE. URL: https://cve.mitre.org/.

Выявление и исправление уязвимостей исключает соответствующие им угрозы и собственно инциденты (компьютерные атаки). Таким образом, методы повышения безопасности систем, ориентированные на уязвимости и дефекты программ, имеют фактически априорный характер, и, соответственно, имеют ряд преимуществ относительно «реактивных» методов, ориентированных на уже произошедшее событие или инцидент безопасности (рисунок 2.3).

Рисунок 2.3. Концептуальная модель компьютерной атаки, реализующей уязвимость



Источник: OWASP Top Ten. URL: https://owasp.org/www-project-top-ten/.

2.1.2. Проблематика уязвимости программ

В связи с развитием информатизации международного общества наблюдается смещение сферы национальных, в том числе военных, активов и коммуникаций в область пространства ИКТ. В настоящее время ряд государств приняли концепцию киберпространства как пятого театра военных действий и обозначили создание вида кибервойск, при этом «около 120 стран мира отрабатывали навык ведения кибервойны» [35] . Соответственно, в области международной безопасности весьма актуальным становится исследование проблематики прогнозирования, предупреждения и сдерживания международных конфликтов в киберпространстве.

Развитие киберконфликта проходит несколько открытых и латентных фаз. В части, касающейся безопасности программных сред и систем, можно выделить три фазы:

- выявление уязвимостей и проработка возможности их реализации с целью проведения кибератак различного назначения;
- обнаружение и реагирование на инциденты, как правило, связанные с проводимыми кибератаками;
- ликвидация последствий успешных кибератак.

Последние две фазы касаются, главным образом, вопросов ситуационного и кризисного менеджмента, и именно им уделяется основное внимание в рамках недавно инициированных международных переговоров и инициатив по проблеме международной безопасности в области киберпространства. В то же время начальная фаза киберконфликта, напрямую связанная с безопасностью программ, в

[35] Андрей Крутских: более 120 стран мира отрабатывали навык ведения кибервойны. Международная жизнь // https://interaffairs.ru/news/show/22362.

области международного права мало изучена и отдана на откуп, главным образом, техническому регулированию, которое в разных странах имеет национальные или фрагментарно межгосударственные черты. Более того, в области международного технического регулирования накопился ряд противоречий, связанных с недоверием к безопасности программной продукции, в разработке или испытаниях которой приняли участие компании иных стран. Иначе говоря, разрешение указанной проблемной ситуации имеет важное значение в области международной безопасности, носит строго предупредительный характер и отвечает целевой задаче повышения доверия к безопасности программных систем в контексте международной безопасности в сфере ИКТ.

2.1.3. Безопасность программ в контексте МИБ

Необходимо указать на два фактора МИБ, касающихся именно безопасности программных систем:

1) критическая структурная сложность программ обусловливает рост техногенного риска;

2) использование ИКТ расширило спектр преднамеренных угроз, а именно в части удаленных (в том числе скрытых и недоказуемых) компьютерных атак, а также угроз компрометации данных сверхбольшого объёма.

Главной причиной техногенного риска является чрезвычайно высокая структурная сложность программ по сравнению, например, с аппаратными или организационно-техническими системами. К примеру, длина исходного текста операционной системы с приложениями на языке высокого уровня может достигать 5-20 Гб, то есть, соответственно, число логических операторов (узлов графа программы) может составлять порядка десятка миллионов, что находится весьма далеко за рамками когнитивных способностей человека-программиста или тестировщика. Опыт показывает, что многие специалисты в области безопасности программных систем психологически абстрагируются и бессознательно не понимают масштабы «проклятия размерности» структуры программы. Для иллюстрации указанного приведём возможности исчерпывающего тестирования тривиальной программной процедуры-функции (таблица 2.1).

Таблица 2.1. Пример 1

Дано:	Процедура-функция умножения двух 32-разрядных чисел
Гипотеза:	Эксперт тратит 1 секунду для контроля правильности результата
Найти:	Временные трудозатраты на выполнение полнофункционального тестирования на всех комбинациях входных данных
Решение:	$N=2^{32+32}$ $T=N \times 1$ с. = 18446744073709551616 с. ≈ 584, 9 трлн. лет

Источник: таблица построена автором.

Что касается второго фактора МИБ, то именно он является причиной становления пятого театра военных действий в киберпространстве. Подавляющее большинство современных компьютерных атак основано на использовании

уязвимостей, при этом атакующему достаточно найти всего одну уязвимость в программном обеспечении, чтобы реализовать соответствующие ей угрозы.

2.1.4. Значимость уязвимости программ

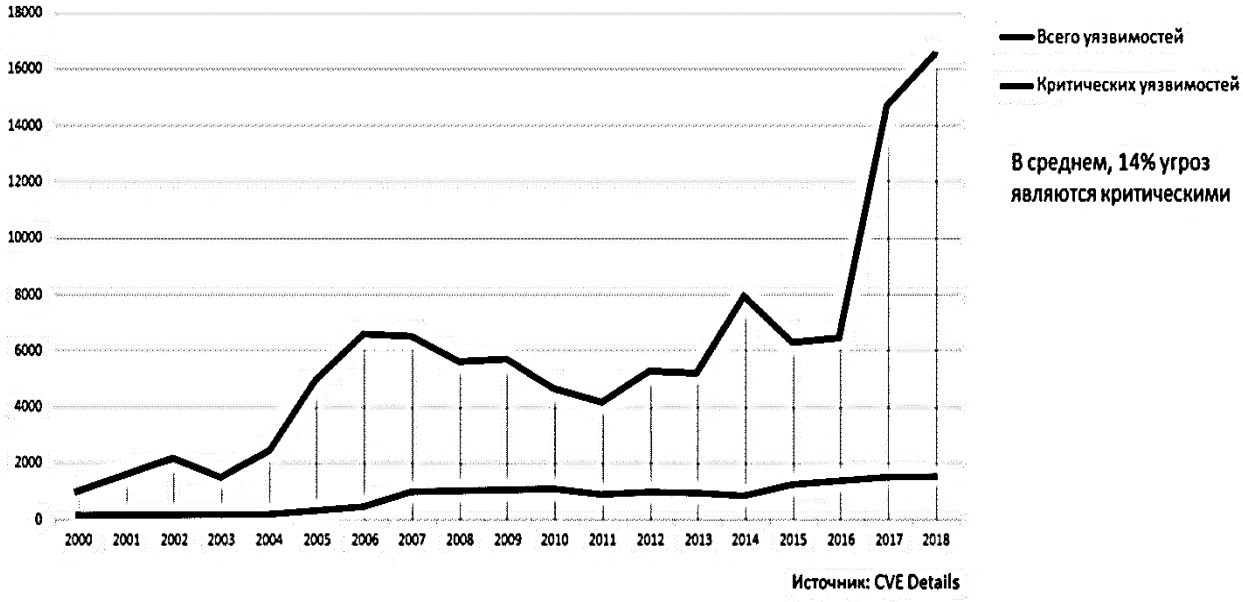
Отмечая уязвимость программных систем, целесообразно отметить, что, несмотря на усилия разработчиков, число ошибок и уязвимостей не снижается (рисунок 2.4), пространство угроз и вызовов в сфере ИКТ находится в постоянной динамике, а отдельные ошибки или уязвимости приводят к крупным авариям и катастрофам (таблица 2.2). Добавим, что объем открытой международной базы уязвимостей Mitre CVE превышает 110 000 уязвимостей, а объем российской базы БДУ ФСТЭК России, ориентированной на внутренний рынок, – 20 000 уязвимостей.

В ситуации с объективным наличием уязвимостей в программном обеспечении и сложностью их обнаружения многие крупные игроки на рынке программных средств (Facebook, Google, Yandex, Microsoft, Министерство обороны США и другие) пытаются максимально воспользоваться услугами краудсорсинга, проводя открытые конкурсы по выявлению уязвимостей (так называемые bug bounty). Так, компания Google потратила $12 млн. на выплаты за найденные ошибки и уязвимости, а министерство обороны США провело уже пять конкурсов Hack the Pentagon, в рамках которых только в 2018 году этичные хакеры представили около ста отчетов об уязвимостях в программных ресурсах автоматизированных систем управления (АСУ) военного назначения США. Ничего удивительного, что вопросы уязвимости программ затронули и «черный рынок», и шпионские скандалы. Наиболее резонансным в позапрошлом году был инцидент с «утечкой» windows-уязвимости из базы данных АНБ США, которую использовала вредоносная программа – криптовымогатель *WannaCry (Wanna Decryptor)*, что, кстати, признали официальные лица корпорации *Microsoft*.

Как известно, вредоносная программа *WannaCry* только за полмесяца инфицировала (нелегитимно зашифровала ресурсы) 500 тыс. компьютеров по всему миру, причем, среди жертв были МИД России, РЖД, оператор мобильной связи «Мегафон» и др.[36] Собственно, в компании *Microsoft* узнали об уязвимости от доброжелателей, пожелавших остаться анонимными. В бюллетене Microsoft MS17-010 также отсутствует какая-либо информация о благодарностях за сообщение об уязвимости, которую использовала вредоносная программа *WannaCry*.

[36] Эпидемия шифровальщика WannaCry: что произошло и как защититься // Kaspersky Lab. 2017ю 13 мая. URL: https://www.kaspersky.ru/blog/wannacry-ransomware/16147/.

Рисунок 2.4. Рост количества уязвимостей в базе MITRE CVE



Источник: cve.mitre.org.

Таблица 2.2. Пример цены ошибки в программном обеспечении

Событие	Краткое описание	Прямой ущерб
Ошибка в программе NASA's Mars Climate Orbiter	Потеря космического спутника из-за ошибочной конвертации единиц измерения	Более $125 млн.
Сбой при открытии 5 терминала аэропорта Хитроу в Лондоне	Функциональная ошибка при возвращении багажа	Более 500 рейсов было отменено, потеря в течение 10 дней 42 000 единиц багажа
Ошибка в программе The Mariner 1 Spacecraft	Потеря космического корабля из-за ошибки в коде – программист пропустил дефис	Более $18 млн.

Источник: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html.

2.1.5. Безопасность программ в контексте стратегической стабильности

Следует отметить связь программной безопасности не только с международной информационной безопасностью, но и со стратегической стабильностью. В качестве резонансных примеров можно привести связанные с тематикой инциденты прошлого года, а именно: доступ прокитайских хакеров к ресурсам спутников США, которые по утверждению *Symantec* внедрили программную закладку в системное ПО СУ, что позволило, якобы, изменить орбиты

спутников и перехватить чувствительные данные[37]. Хронологии кибероперациий, связанных с инцидентами в ядерной области, описаны в различных источниках.

2.1.6. Зарубежные исследования в области безопасности программ

Проблематика безопасности программных продуктов и систем является весьма востребованной, об этом свидетельствуют как современные тенденции в области международной сертификации защищённых программных изделий[38], так и соответствующие изыскания DARPA (таблица 2.3).

Таблица 2.3. Исследования DAPRA по тематике уязвимостей программ

Поисковые исследования	Целевое назначение
Vetting Commodity IT Software and Firmware (VET)	Контроль недекларированных возможностей и закладок в программном обеспечении периферийных устройств (факсов, принтеров, телефонах и пр.)
Automated Program Analysis for Cybersecurity (APAC)	Создание средств автоматизации выявления недекларированных возможностей и закладок в программном обеспечении мобильных платформ (Android)
Cyber Grand Challenge (CGC)	Академические соревнования по выявлению уязвимостей
Clean-slate design of Resilient, Adaptive, Secure Hosts	Создание методов и инструментальных средств (среда разработки, среда верификации, среда выполнения) создания компьютерных систем, устойчивых к компьютерным атакам
Mining and Understanding Software Enclaves	Повышение надежности программного обеспечения, в том числе создание техник и средств верификации и статического анализа исходного кода программ

Источник: Defense Advanced Research Projects Agency. URL: www.darpa.mil.

2.1.7. Запретительные меры в области регулирования безопасности программ

Актуальность киберугроз и соответствующих вызовов международной информационной безопасности и стратегической стабильности подразумевает активизацию инициирования и соблюдения договорных международных процессов в сфере ИКТ. Однако в мировом сообществе вместо консолидации в области

[37] Menn J. China-based campaign breached satellite, defense companies: Symantec // Reuters. 2018. 19 June. URL: https://www.reuters.com/article/us-china-usa-cyber/china-based-campaign-breached-satellite-defense-companies-symantec-idUSKBN1JF2X0.

[38] Barabanov A., Markov A. Modern Trends in the Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria // Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015. P. 30-33. DOI: 10.1145/2799979.2799980.

повышения доверия к безопасности программ пока доминируют «запретительные» меры, например,

- в Европе наблюдается противоречие между требованиями по коллаборативной сертификации (на основе коллаборативных профилей защиты) и требованиями Евросоюза или отдельных национальных государств;
- в США введено ограничение на использование программной продукции, прошедшей сертификацию в Китае и России. В свою очередь Китай и Россия реализуют ассиметричные меры;
- ряд стран проводят политику импортозамещения, ведут черные списки поставщиков иностранной продукции или вводят ограничения по использованию импортной продукции и др.

Что касается России, то наиболее ярко это демонстрируют два последних события прошедшего года:

- запрет на использование продукции компании «Лаборатория Касперского» в государственных учреждениях ряда западных стран;
- запрет на использовании в течение пяти лет в государственных учреждениях США американских программных средств, прошедших сертификацию с предоставлением программных исходных кодов в России и др.

Несмотря на то, что такая политика оправданна в определённых геополитических условиях, она мало конструктивна в плане повышения международной интеграции и безопасности по целому ряду проблемных вопросов – к примеру, противоречит консолидации стран по противодействию нелегитимной деятельности третьих сторон, в первую очередь криминального хакерского сообщества.

2.2. Пути повышения доверия к безопасности программ

Повышение доверия к безопасности программных систем создает объективную доверенную платформу для снижения уровня угроз, рисков и в конечном счете инцидентов в киберпространстве. Могут быть предложены следующие пути повышения безопасности программных систем в контексте международной информационной безопасности:

- правовое регулирование безопасности программ, включая обеспечение осведомленности об уязвимостях;
- техническое регулирование безопасности программного обеспечения, включая международную оценку соответствия (сертификацию) программных продуктов и систем управления (менеджмента) производством программ.

Правовое регулирование (как общее регулирование) должно устанавливать отношения в сфере безопасности ИКТ, а техническое регулирование (как специальное регулирование) должно устанавливать отношения в технической сфере по вопросам безопасности ИКТ. Целевые установки правового регулирования частично заложены в российских инициативах глобального характера, в том числе в ранее указанном своде 13 международных правил, норм и принципов ответственного поведения государств, рекомендованном Резолюцией Генеральной Ассамблеи ООН A/RES/73/27 и поддержанном 139 странами. Что касается технического регулирования, то в мировой практике сложились системы международной и межгосударственной стандартизации и сертификации, гармонизированные с российскими нормативно-правовыми актами. В то же время,

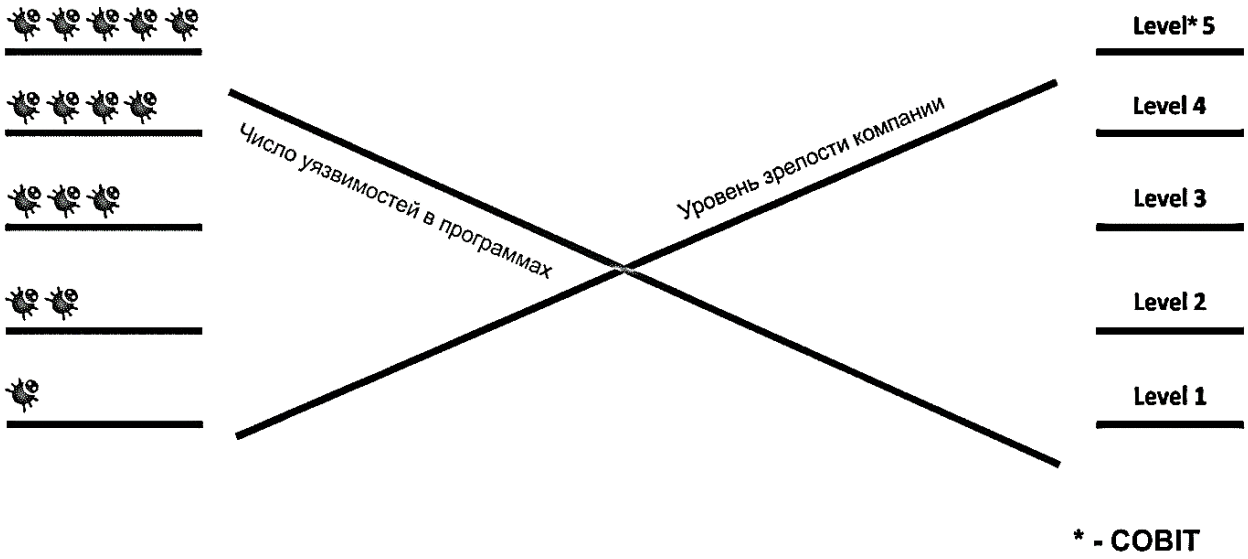
очевидно, что и правовое, и техническое регулирование международной информационной безопасности в сфере ИКТ находятся на начальном этапе формирования, отдельные вопросы которого рассмотрены в данной главе, а именно:

1) повышение зрелости международных предприятий-разработчиков программ.
2) повышение уровня достоверности результатов сертификации программных средств защиты информации с предоставлением доступа к исходным текстам на этапе испытаний.

2.2.1. Регулирование разработки безопасных программ

Статистика испытательных лабораторий показала, что основной причиной уязвимостей программного обеспечения является низкая зрелость компаний-разработчиков, игнорирующих меры безопасности, связанные с проектированием, разработкой, производством, внедрением, поставкой и сопровождением программных продуктов. Так, авторами получена статистика, что уровень менеджмента (или зрелости [39]) компании существенно влияет на уровень безопасности разработанного, изготовляемого или поставляемого программного обеспечения, а именно на степень отсутствия уязвимостей и возможности оперативного их исправления в случае выявления. Исследования испытательных лабораторий показали строгую обратную пропорциональность общего числа уязвимостей уровням зрелости компании-разработчиков программ (рисунок 2.5). По заявлению компании *Microsoft*, число уязвимостей в программном обеспечении снизилось более чем на 80% при введении соответствующей подсистемы менеджмента (*Microsoft Secure Software Development Life Cycle*).

Рисунок 2.5. Закон обратной пропорциональности «5 на 5» обратной пропорциональности зрелости компании и количества уязвимостей в программной продукции



Источник: рисунок построен автором.

[39] Effective IT Governance at Your Fingertips // Information Systems Audit and Control Association (ISACA). URL: https://COBITonline.isaca.org/.

Зачастую угрозы программной безопасности связаны не только с разработчиком, но также изготовителем и поставщиками. Иначе говоря, компьютерная атака на программные ресурсы организации может быть проведена на различных этапах жизненного цикла программ. Наиболее популярными в настоящее время являются компьютерные атаки на логистическую цепочку (supply chain attack), цель которых состоит в компрометации наименее защищенных объектов в цепочке поставок. При этом компрометации могут быть подвергнуты программные ресурсы не только конечного заказчика, но также всех участников цепочки поставки. Атака реализуется через внедрение вредоносного программного обеспечения или программно-аппаратного имплантата в решения, используемые организацией (рисунок 2.6).

Для иллюстрации размера бедствия на начальном этапе создания программ на рисунке 2.7 приведена статистика распределения разработчиков программ в зависимости от привлечения сторонних организаций к разработке.

Известными примерами указанных атак являются компрометация инструментов разработки программного обеспечения, кража сертификатов или подписание вредоносного программного обеспечения с помощью сертификата разработчика, компрометация встроенного микрокода, инсталляция вредоносного программного обеспечения на устройства (камеры, устройства USB, телефоны) и др.

Одним из недавних громких случаев, касающихся целенаправленных атак на логистическую цепочку, является кибероперация *ShadowHammer*. В рамках кибероперации вредоносная программа была внедрена в легитимную утилиту ASUS Live Update. Атака была адресно направлена на избранную группу пользователей, строго определенных по MAC-адресам личных сетевых адаптеров. Из более чем 200 вредоносных образцов, участвовавших в этой атаке, удалось извлечь более 600 уникальных MAC-адресов. Наибольший процент адресных данных касался России.

На уровне систем менеджмента к основным мерам по минимизации рисков подверженности атакам на цепочку поставок, предпринимаемых разработчиком и поставщиками, являются:

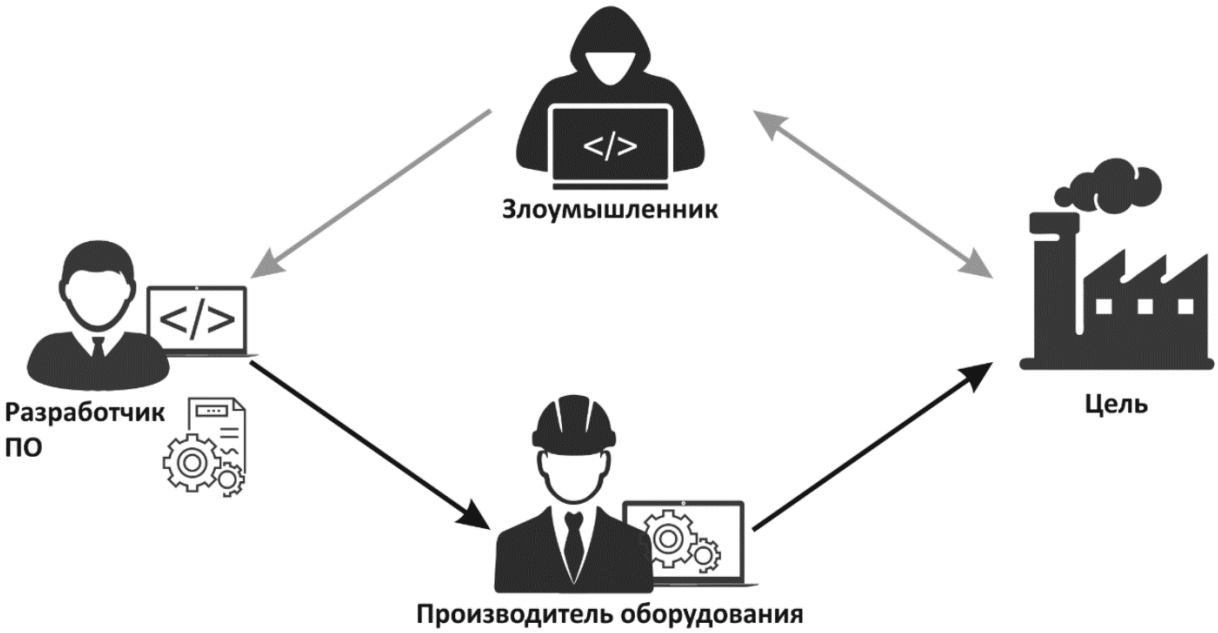
- внедрение процессов безопасной разработки;
- внедрение системы менеджмента информационной безопасности (например, в соответствие со стандартом ISO/IEC 27001).

На уровне отдельных процессов к основным мерам безопасности относят: тестирование на проникновение, аудит безопасности кода, контроль используемых сторонних компонентов и др.

В настоящее время известен ряд руководств («хороших практик») и стандартов международных и национальных организаций, касающихся разработки безопасных программ, например, Microsoft SDL, Cisco SDL, BSIMM, рекомендации Министерства обороны США, ISO/IEC 27034, ISO/IEC TR 24772 и др. В литературе хорошо проработаны угрозы цепочкам поставок, в то же время непреднамеренные угрозы, а также угрозы иных подэтапов жизненного цикла программ зачастую описаны недостаточно полно. Имеющиеся международные стандарты не обеспечивают полноту регламентации всех процессов и процедур разработки программ с учетом современного спектра угроз информационной безопасности.

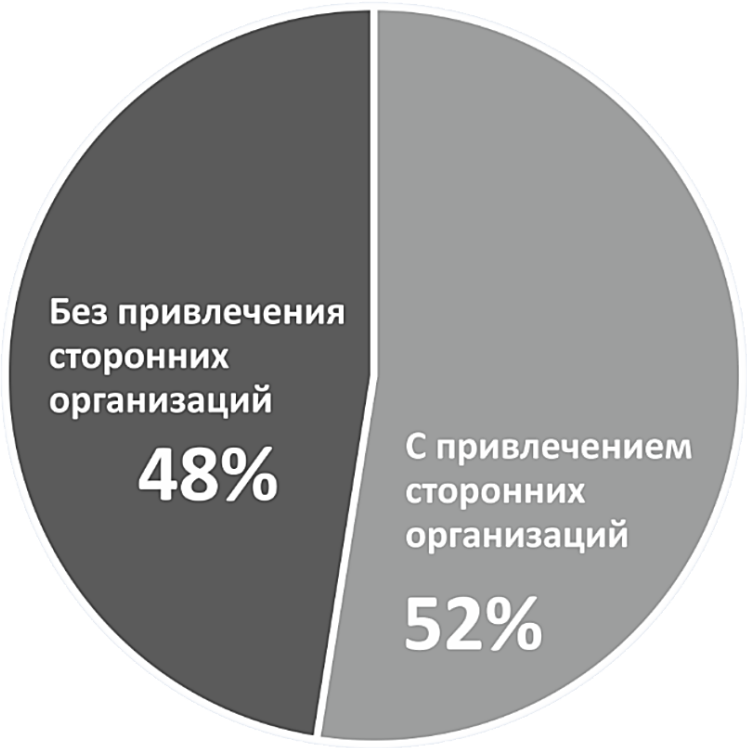
В таблицах 2.4 и 2.5 показаны фрагменты анализа нормативных документов в области создания безопасных программ, что демонстрирует отсутствие полноты зарубежных исследований.

Рисунок 2.6. Концептуальная модель атаки на цепочку поставки



Источник: The MITRE Corporation. URL: mitre.org.

Рисунок 2.7. Статистика привлечения сторонних организаций при программировании



Источник: State of software development in 2018 // Coding Sans LTD. URL: https://codingsans.com/state-of-software-development-2018.

Таблица 2.4. Каталоги угроз, связанные с жизненным циклом программ

Каталог угроз, связанных с жизненным циклом программам	Учет угроз, специфичных среде разработки	Учет непреднамеренных угроз
MITRE&DSE	+	-
NIST SP 800-30 rev.1	-	-
NIST IR 8144	+	-
MITRE CAPEC	+	-
БДУ ФСТЭК России	-	+

Источник: таблица построена автором.

С целью обеспечения полноты учета процессов разработки программ, мер безопасности и соответствующих угроз информационной безопасности (при разработке и поставке программ) техническим комитетом по стандартизации России ТК-362 «Защита информации» разработан и введен в действие национальный стандарт по созданию безопасных программ – ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», а также инициирована разработка линейки связанных с ним стандартов. Идея национального стандарта и аспекты его гармонизации, а также схема гармонизации указанного стандарта с международными стандартами представлены на рисунках 2.8 и 2.9 соответственно.

Целью создания линейки стандартов по разработке безопасных программ является предотвращение появления уязвимостей программ и их устранение. При этом прослеживается связь между процессами конструирования (что регламентировано ГОСТ Р ИСО/МЭК 12207) и мерами по безопасной разработке, которые выбираются с учетом риск-ориентированного подхода, т.е. с учетом актуальных угроз. Меры безопасности в стандарте разделены на три группы (реализации программ, поддержки программ, организационного обеспечения) и включают в себя девять основных процессов:

- анализ требований;
- проектирование архитектуры;
- конструирование;
- квалификационное тестирование;
- управление документацией и конфигурированием;
- решение проблем в процессе эксплуатации;
- поддержка приемки;
- управление инфраструктурой среды разработки;
- управление персоналом.

Взаимосвязь процессов и основных мер безопасности представлена на рисунках 2.10 и 2.11.

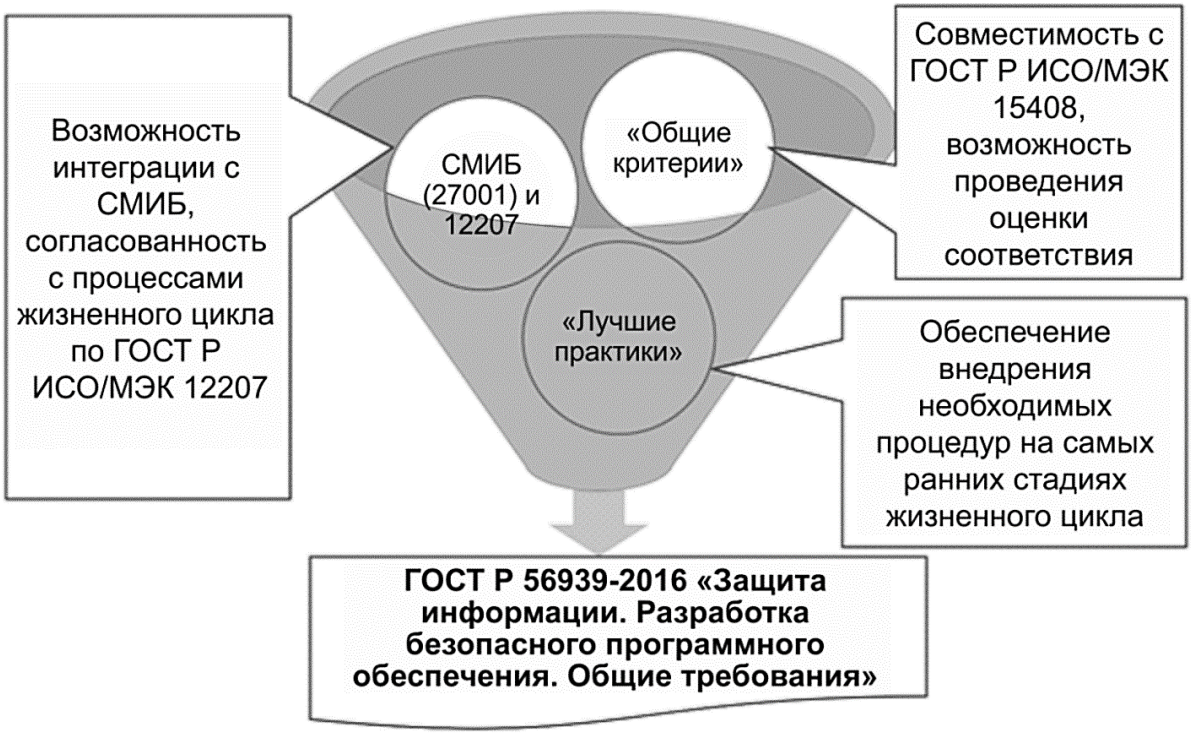
Таблица 2.5. Нормативные документы по разработке безопасных программ

Характеристика, наличие мер по разработке безопасного программного обеспечения	Стандарт/руководство					
	ISO/IEC 15408	Microsoft SDL	Open SAMM	OWASP CLASP	ISO/IEC TR 24772	ISO/IEC 27034-1
Обучение сотрудников	-	+	+	-	-	-
Обеспечение безопасности инфраструктуры	+	-	-	-	-	-
Управление конфигурацией разрабатываемых программ	+	-	-	-	-	-
Моделирование угроз безопасности информации, источником которых являются программы	+	+	+	+	-	-
Определение требований в части разработки безопасных программ	+	+	+	+	-	-
Использование стандарта оформления исходного кода	-	+	+	+	+	-
Проведение статического анализа исходного кода	-	+	+	+	-	-
Проведение динамического анализа кода	-	+	+	+	-	-
Проведение экспертизы исходного кода программ в ручном режиме	-	+	+	+	-	-
Проведение анализа уязвимостей	-[40]	+	+	+	-	-
Обеспечение безопасности поставки	+	+	+	-	-	-
Устранение выявляемых при эксплуатации уязвимостей	+	+	+	+	-	-
Возможность использования документов при сертификации	+	-	-	-	-	-
Наличие методики выбора подмножества мер разработки	+	+	+	-	-	+
Согласованность с процессами жизненного цикла программ (согласно ISO/IEC 12207)	-	-	-	-	-	+

Источник: таблица построена автором.

[40] Стандарт ISO/IEC 20004 определяет подход к обнаружению уязвимостей при оценке соответствия ИТ-продуктов с учетом ISO/IEC 15408.

Рисунок 2.8. Концептуальная модель формирования стандарта по разработке безопасных программ

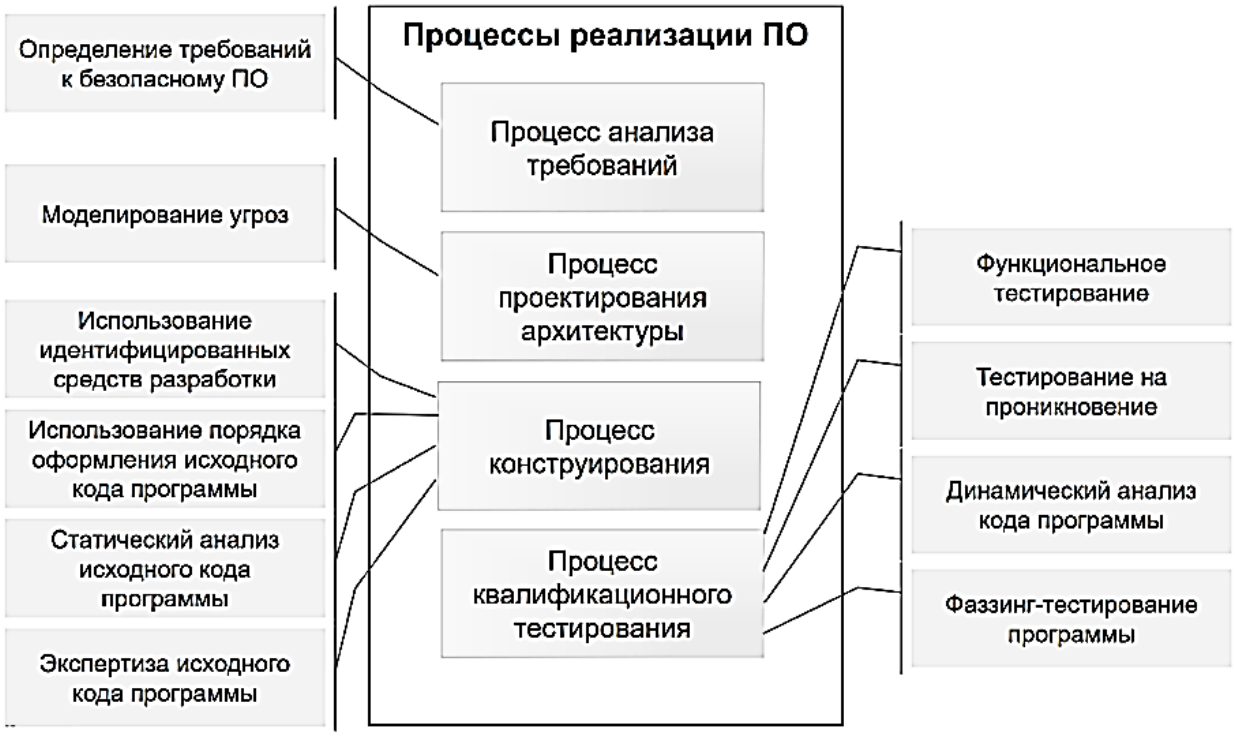


Источник: рисунок построен автором.

Рисунок 2.9. Гармонизация стандарта по безопасной разработке

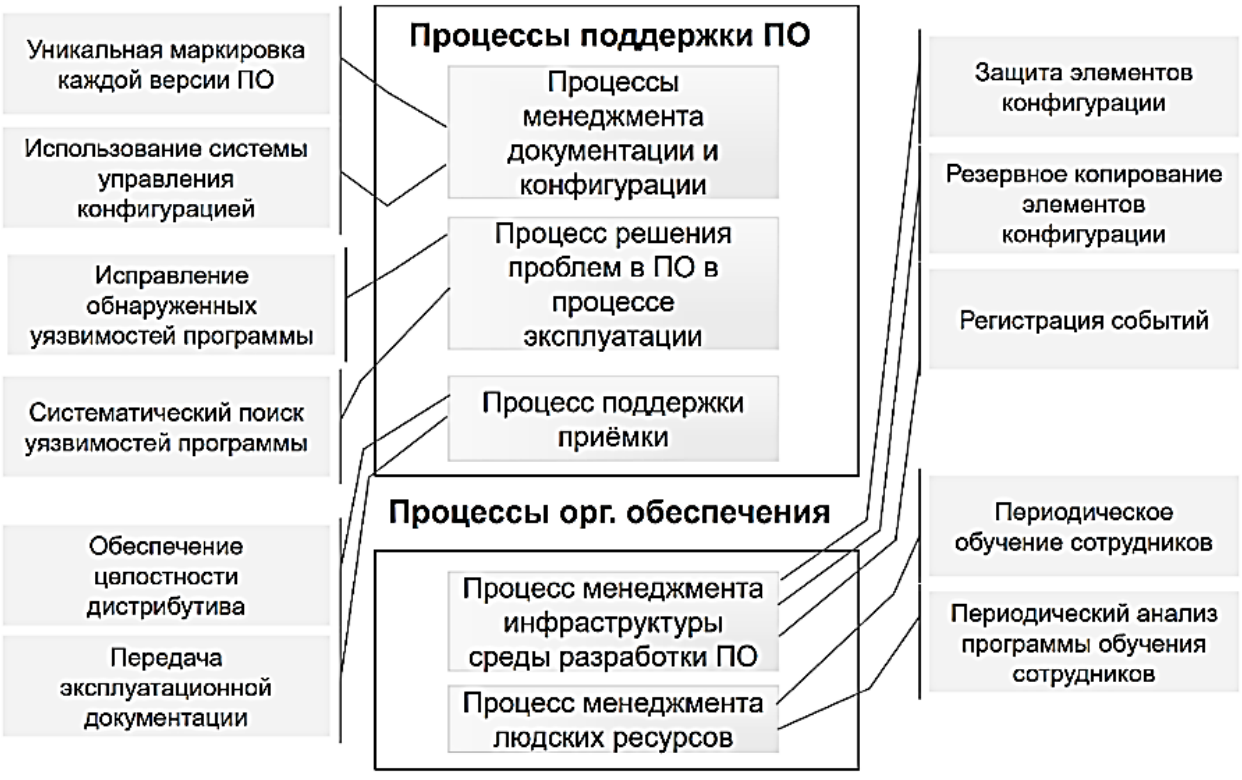
Источник: рисунок построен автором.

Рисунок 2.10. Меры по реализации безопасных программ



Источник: рисунок построен автором.

Рисунок 2.11. Меры по поддержке и обеспечению безопасных программ



Источник: рисунок построен автором.

2.2.2. Регулирование оценки соответствия программ требованиям по безопасности информации

Оценка соответствия в области информационной безопасности обычно проходит в форме обязательной сертификации средств защиты информации по требованиям безопасности информации, цель которой в итоге состоит в сведении к минимуму риска эксплуатации уязвимостей в программном обеспечении. Для пояснения результативности, эффективности и ограничений методов и техник сертификационных испытаний приведем классификацию подходов к тестированию и искомых дефектов и уязвимостей.

В самом общем плане методы тестирования классифицируются следующим образом:

- по жизненному циклу: верификация, анализ кода и тестирование программ;
- по запуску: статический анализ и тестирование (динамический анализ);
- по наличию исходного кода: метод «черного ящика» (например, функциональное тестирование) и метод «белого ящика» (структурное тестирование).

Выбор метода и методики зависит от цели тестирования, то есть от класса выявляемых дефектов и уязвимостей. Выявляемые классы в общем виде можно разделить на:

- непреднамеренные и преднамеренные;
- нефункциональные и функциональные;
- известные, подобные известным и неизвестные.

При этом преднамеренные уязвимости, в частности, программные закладки, связаны с комбинациями редко используемых входных данных, когда стохастические методы мало результативны.

В следующем случае классификации легко показать, что функциональные уязвимости (особенно комбинированного типа) синтаксически корректны, то есть их в принципе невозможно искать методами проверки правильности кода подпрограмм (не говоря уже про дедуктивную верификацию нескольких строк кода) без корректных функциональных спецификаций. Разительное отличие существует между трудоемкостью выявления известных уязвимостей и неизвестных уязвимостей. Очевидно, что проверки наличия известных уязвимостей путем тривиального сканирования или же известных компьютерных вирусов с помощью средств антивирусной защиты целесообразно относить не к сертификационным испытаниям (то есть не к этапу внедрения), а к менеджменту поддержки эксплуатации и сопровождения программ, так как они имеют силу исключительно применительно к временной точке эксплуатации. Легко заметить, что выбор класса дефектов определяет подходы к тестированию программ, часть из которых относятся к области теории надежности (когда основным фактором является отказ или проявляемая ошибка), а часть – к теории информационной безопасности. Оплошности в подобной классификации приводят к подмене понятий с вытекающими негативными последствиями в области сертификации и информационной безопасности.

Что касается испытаний в области информационной безопасности, то наиболее известными в литературе техниками проверки программ являются:

- прикладная (алгоритмическая) верификация;
- инспекция кода;
- статический декомпозиционный анализ (выявление недекларированных возможностей путем сбора и анализа маршрутов);
- статический сигнатурно-эвристический анализ;

- динамический структурный анализ и отладка;
- функциональное тестирование («черный ящик», детерминированный подход);
- фаззинг («черный ящик», стохастический подход);
- тестирование на проникновение (выявление и эксплуатация уязвимостей) и пр.

При различных достоинствах и недостатках указанных подходов можно констатировать, что на сегодня нет универсального метода. Так, например,

- парольную закладку легко найти по наличию констант в цикле операции аутентификации, логическую бомбу – по счетчику;
- сбой и отказ в обслуживании может быть зафиксирован в процессе фаззинг-тестирования или стресс-тестирования;
- некорректности кодирования, как правило, выявляются на этапе компиляционного разбора.

В настоящее время подходы к выявлению уязвимостей известного типа с учетом открытых источников опираются на концептуальный подход ISO/IEC TR 20004. Кроме все прочего, в мировой практике известны руководства, ориентированные на тестирование приложений (например, NIST SP 800-163, OWASP MSP и пр.), тестирование на проникновение и аудит (PTES, OWASP ASVSP и др.).

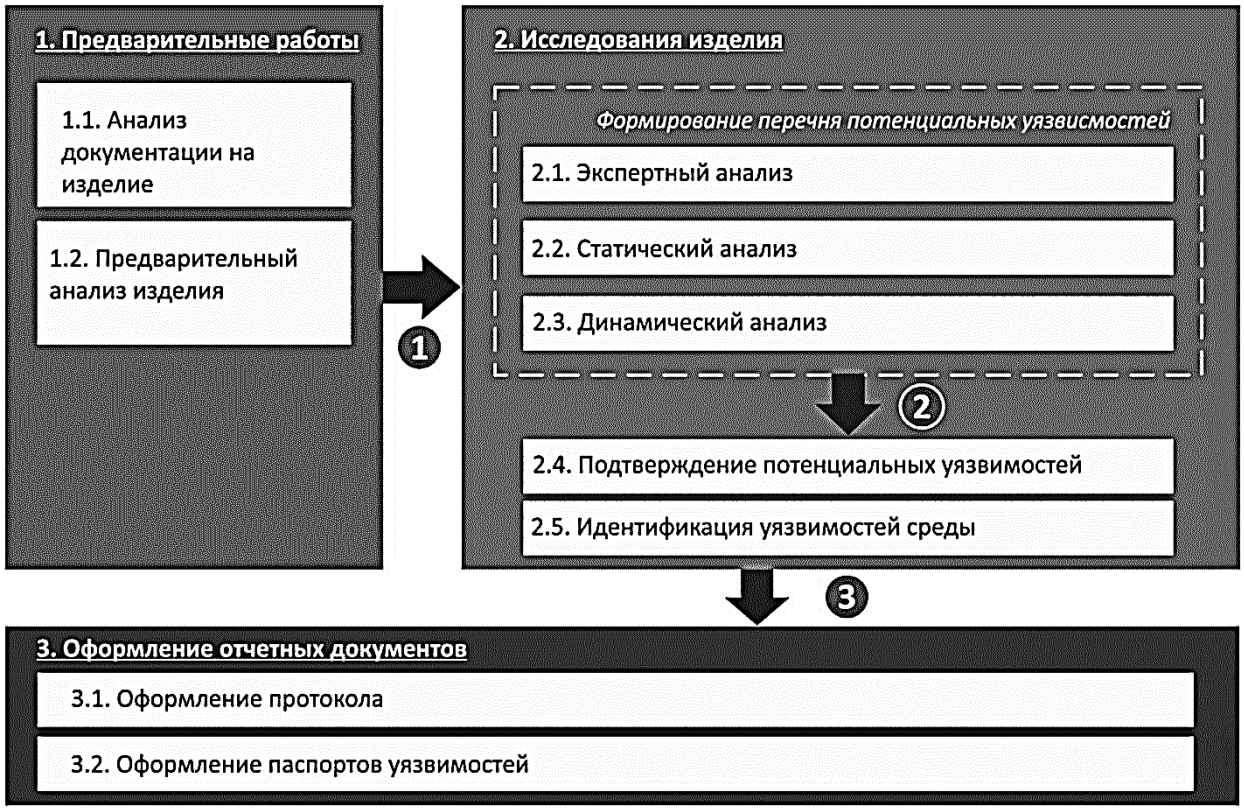
В России сейчас проходит апробацию комплексный подход к проверке безопасности программ.

Несмотря на использование множества различных методов и техник проверки программ, невозможно получить допустимый уровень доверия к программным ресурсам без предоставления доступа к исходным кодам. Наиболее наглядно это можно показать на примере «плавающих» ошибок и программных закладок, инициирование которых связано с редкими комбинациями входных данных, т.е. их невозможно найти методами тестирования по принципу «черного ящика», например, фаззинг-тестированием. Иначе говоря, только доступ к исходным текстам программ дает некоторую вероятность обнаружения любой уязвимости за счет экспертных знаний. На рисунках 2.12 и 2.13 приведены статистика по результативности базовых методов анализа безопасности программ, которая подтверждает ведущую роль эксперта и предпочтительность наличия исходных кодов и спецификаций, а также результативность различных методов выявления уязвимостей соответственно.

Таким образом, можно сделать два вывода:

- эффективность проверки безопасности программ в значительной степени зависит от квалификации экспертов, которые принимают решение при оценке степени критичности дефекта, уязвимости и угрозы;
- невозможно обеспечить допустимый уровень доверия к безопасности программ без предоставления доступа к исходным текстам программ.

Рисунок 2.12. Концептуальная модель выявления уязвимостей в процессе сертификационных испытаний программ



Источник: рисунок построен автором.

Рисунок 2.13. Результативность различных методов выявления уязвимостей

Источник: По опыту работы НПО «Эшелон».

2.2.3. Международные аспекты организации доступа с исходному коду программ

К сожалению, доступ к исходным текстам программных систем является весьма дискутируемым моментом. Критика политического толка в итоге приводит к указанным ранее запретительным мерам в области интеграции международного общества с целью обеспечения необходимого уровня международной информационной безопасности. Наиболее ярким запретительным политическим актом является закон об обороне США 2019 г. №115-232, не разрешающий использовать американские ИТ-продукты в оборонной сфере, если они были сертифицированы в течение последних 5 лет с предоставлением исходного кода в иностранных государствах.

Следует указать, что на политическом уровне очевидна подмена понятий «открытие кода» и «организация доступа к коду на период испытаний». Рассмотрим этот момент подробнее. Открытие кода как такового, разумеется, несет угрозы раскрытия информации об уязвимостях и компрометации интеллектуальной собственности. Однако скрытие уязвимостей кода на межгосударственном уровне в целях обеспечения наступательного информационного противоборства сразу же дискредитирует любое доверие к компьютерным системам и продуктам между конкретными странами и сводит на нет любые международные договоренности.

На промышленном или коммерческом уровне основными угрозами, которые видят компании-разработчики, является угроза кражи интеллектуальной собственности, а также угроза нелегитимного открытия информации об уязвимостях иным сторонним лицам. В то же время опыт работы испытательных лабораторий показывает, что давно известно решение, обеспечивающее строгое выполнение требований по безопасности кода, а именно создание автономного защищенного стенда в защищенном помещении или «пустой комнаты» (clean room). В таком помещении на территории заказчика (под контролем службы безопасности заказчика) организуется доступ к исходному коду программ именно *на период* испытаний. В рамках данного доступа в закрытой защищенной среде выполняется сборка программы, фиксируется ее целостность (контрольные суммы) и проводятся необходимые оговоренные проверки. Разумеется, без согласования со службой безопасности заказчика не допускается вынос какого-либо носителя информации, инициирование сеанса связи вовне и прочее. Все документальные подтверждения проведенных проверок и выводы обсуждаются и утверждаются заказчиком. В итоге, в случае обнаружения уязвимости, получается следующее: заказчик исправляет уязвимость и согласует отчетные материалы – или заказчик блокирует оформление отчетных материалов (в этом случае он не получает сертификат). При этом публичные действия испытательной лаборатории ограничены соглашением о неразглашении (со штрафными санкциями), то есть учтены возможные риски заказчика.

Указанный подход характеризуется рядом следующих преимуществ и гарантий:

- позволяет повысить безопасность программ за счет консолидации деятельности разработчиков и допущенных заказчиком специалистов испытательной лаборатории;
- выявленные уязвимости будут исправлены в рамках сертификации в обязательном порядке, а информация о об этом не будет известна третьей стороне;

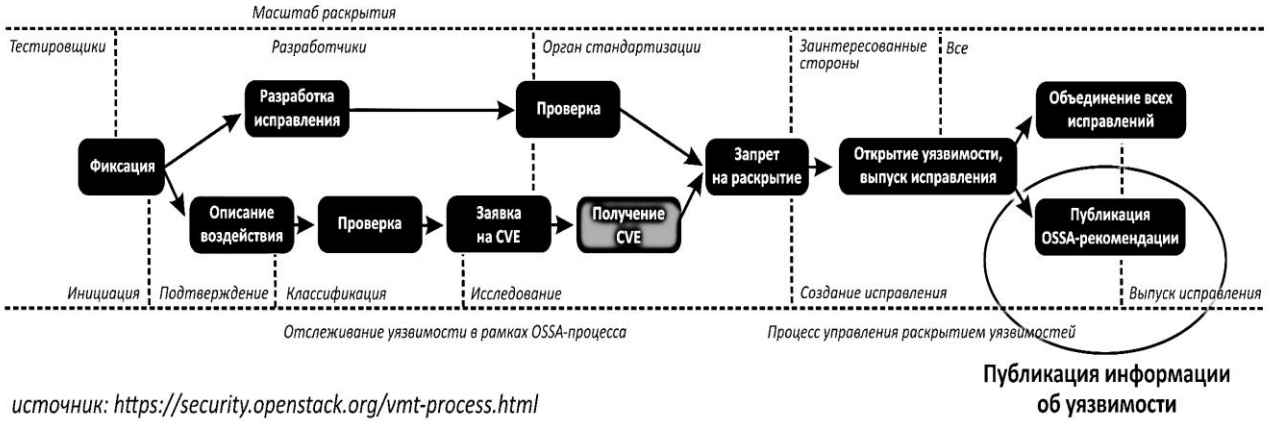
- проверки абсолютно прозрачны, все действия (организация доступа, контроль и мониторинг работы, обсуждение результатов, подготовка отчетных документов и пр.) технически и нормативно обеспечиваются службой безопасности заказчика;
- появляется элемент доверия к программному средству, так как всегда имеется вероятность обнаружить потенциально опасный код (или продемонстрировать его отсутствие), в чем в итоге заинтересованы обе стороны сертификации.

При этом вопросы открытия доступа к исходным кодам для проведения испытаний понятны многим крупным компаниям-разработчикам программ. Так, компания Microsoft открыла доступ к исходному коду своих программных продуктов более, чем в 30-ти странах мира[41], включая Россию. Подразделение компании «Лаборатория Касперского», расположенное в Москве, предложило открыть доступ к исходному коду своих программных средств уполномоченным органам по сертификации США[42].

Однако даже само требование проверки исходных кодов стало предметом политических противоречий между США, подход которых предполагает переход к упрощенным коллаборативным профилям защиты (*collaborative security profile*), и ЕС, усиливающим проверки программ в соответствии с недавним европейским актом о кибербезопасности – EU Cybersecurity Act.

В заключении следует указать на прямую связь между обнаружением уязвимостей и зрелостью компании. Если разработчик имеет зрелые процессы разработки и изготовления, он также публикует информацию об обнаруженных уязвимостях (рисунок 2.14).

Рисунок 2.14. Схема обнаружения и описания уязвимости программного обеспечения



Источник: Openstack. URL: openstack.org.

[41] The Microsoft Transparency Center in Brussels // Microsoft URL: https://blogs.microsoft.com/eupolicy/transparency-center/.

[42] Finkle J., Auchard E. Kaspersky Lab to open software to review says nothing to hide // Reuters. 2017. 23 October. URL: https://www.reuters.com/article/us-usa-security-kaspersky-russia/kaspersky-lab-to-open-software-to-review-says-nothing-to-hide-idUSKBN1CS0Y1.

* * *

Представленный материал позволяет сделать вывод о важной роли безопасности программного обеспечения в сфере международной информационной безопасности. Наиболее перспективными видятся два направления повышения безопасности программ в области международной информационной безопасности:

- исследования в области конвергенции лучших практик в области правового и технического регулирования с учетом предоставления доступа к исходным кодам на этапе испытаний;
- исследования в области менеджмента информационной и кибербезопасности организаций-разработчиков и поставщиков программных систем.

С учетом полученных научных утверждений и динамики сферы ИКТ предлагаются в рамках развития ранее указанного свода международных правил, норм и принципов ответственного поведения государств внесение уточнений в пункты 9 и 11 в следующей интерпретации:

- государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи и поставщики могли быть уверены в безопасности продуктов и услуг в сфере ИКТ;
- государства должны способствовать ответственному представлению информации и факторах уязвимости в сфере ИКТ, делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, а также принимать меры, направленные на исключение и своевременное устранение соответствующих угроз для ИКТ и зависящей от ИКТ инфраструктуры.

ГЛАВА 3.

Суперкомпьютеры и проблемы безопасности

Единое строгое и общепринятое определение «суперкомпьютера» или «супер-ЭВМ» пока не существует. Компания «*Hewlett Packard Enterprise»* предлагает следующую формулировку: *«Термин "суперкомпьютеры" означает системы для выполнения сверхсложных задач или задач, которые задействуют большие объемы данных, за счет концентрации вычислительных ресурсов множества параллельно работающих компьютеров (образующих "суперкомпьютер"). Суперкомпьютеры работают с максимальной эффективностью и производительностью, которая обычно измеряется в петафлопсах. Они часто используются в метеорологии, энергетике, здравоохранении, производстве и других сферах»*[43].

В материале о суперкомпьютере «Фишер», созданном для Объединенного института высоких температур Российской академии наук, «Ростех» определяет *современный суперкомпьютер* как «*огромное устройство, состоящее из модулей памяти, процессоров, плат, объединенных в вычислительные узлы, связанные между собой сетью. Управляющая система распределяет задания, контролирует загрузку и отслеживает выполнение задач. Системы охлаждения и бесперебойного питания обеспечивают беспрерывную работу супер-ЭВМ. Весь комплекс может занимать значительные площади и потреблять огромное количество энергии».*[44]

Российские программисты определяют *суперкомпьютер* как *«очень мощный компьютер с тысячами процессоров, который многократно ускоряет сложные расчёты и обрабатывает петабайты данных. В суперкомпьютере отдельные машины связаны высокоскоростной сетью (интерконнект)»*.[45]

Архитектуру суперкомпьютера можно проиллюстрировать на примере суперкомпьютера «Ломоносов» из МГУ (рисунок 3.1).

Благодаря исключительным объемам обрабатываемой информации и скорости обработки, суперкомпьютеры активно используются и в области безопасности, начиная от задач логистики и заканчивая имитационным моделированием течения процессов в ядерных боезарядах. Их роль в дальнейшем будет только возрастать, следовательно, их место в процессе обеспечения национальной и международной безопасности требует глубокого экспертного анализа.

3.1. Рейтинги суперкомпьютеров

Наиболее распространенной характеристикой производительности суперкомпьютеров является «петафлопс», равный 10^{15} флопсам, где «*флопс» – внесистемная единица, показывающая число операций с плавающей запятой в секунду для данной вычислительной системы*. Рубеж в 1 петафлопс был преодолен в 2008 году суперкомпьютером «*Roadrunner»*, созданным компанией IBM

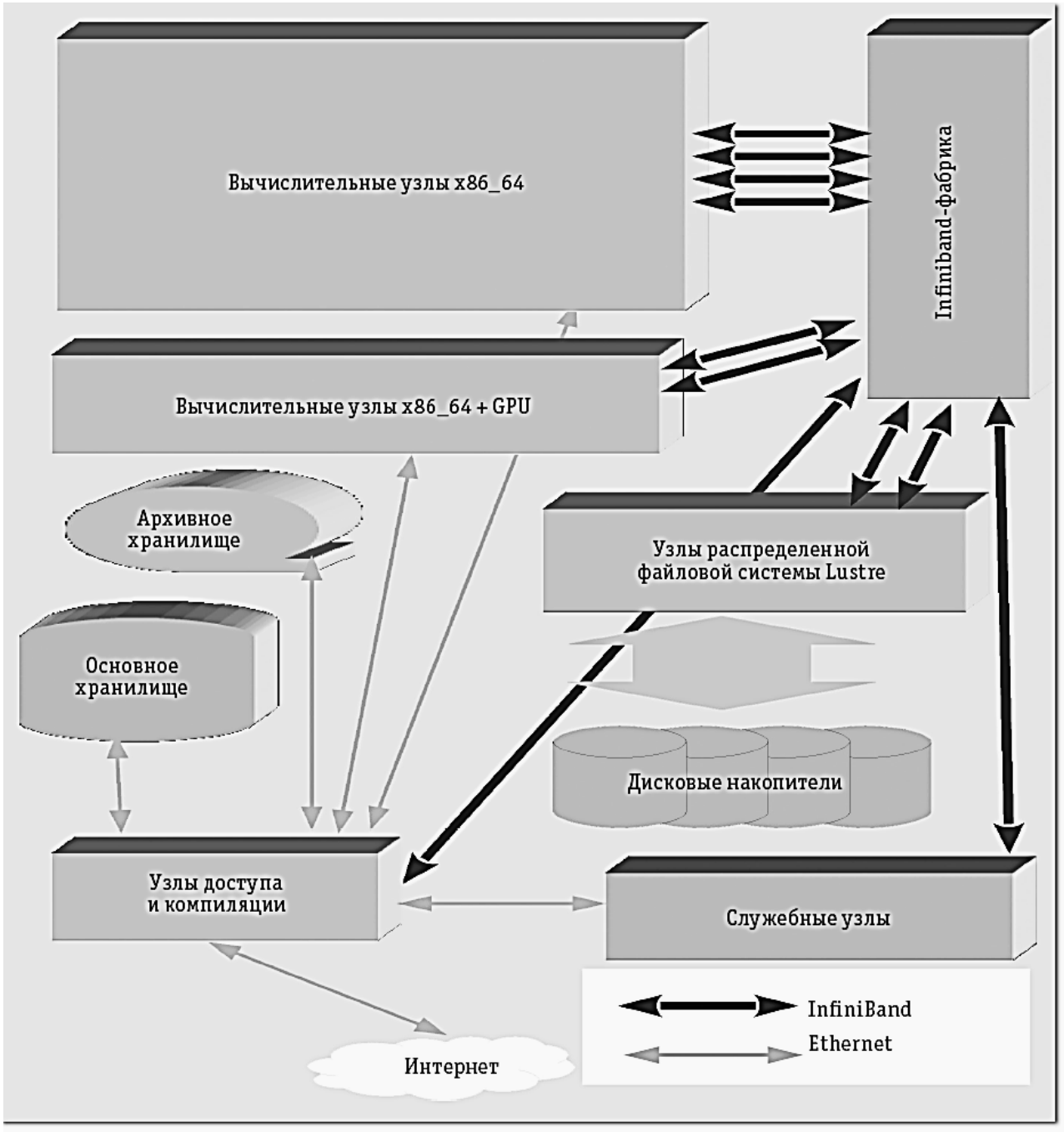
[43] Определение суперкомпьютеров // Официальный веб-сайт Hewlett Packard Enterprise URL: https://www.hpe.com/ru/ru/what-is/supercomputing.html.

[44] Суперкомпьютеры: титаны вычислений // Официальный веб-сайт Ростеха. 2019. 4 октября. URL: https://rostec.ru/news/superkompyutery-titany-vychisleniy//.

[45] Абрамов С. Суперкомпьютеры: обратные рекорды // Наука и жизнь. 2019. № 1. URL: https://www.nkj.ru/archive/articles/35326///.

в интересах Лос-Аламосской национальной лаборатории в Нью-Мексико, США[46]. В ближайшие годы ожидается появление суперкомпьютеров, производительность которых будет измеряться в эксафлопсах, равных 10^{18} флопсов.

Рисунок 3.1. Архитектура суперкомпьютера «Ломоносов»



Источник: В. Воеводин, С. Жуматий, С. Соболев, А. Антонов, П. Брызгалов, Д. Никитенко, К. Стефанов, В. Воеводин. Практика суперкомпьютера «Ломоносов», Открытые системы. СУБД, 2012, № 07.

Лучшие современные суперкомпьютеры, как правило, участвуют в глобальном рейтинге *Linpack Top-500*, который можно считать достаточно репрезентативным. По

[46] Fact Sheet & Background: Roadrunner Smashes the Petaflop Barrier // Официальный веб-сайт IBM. URL: https://www-03.ibm.com/press/us/en/pressrelease/24405.wss.

состоянию на июнь 2020 года [47] наибольшее количество суперкомпьютеров в рейтинге (226 единиц), а также максимальная общая вычислительная мощность приходится на Китай. На втором месте находятся США (113 единиц). В условную «пятерку» входят также Япония, Франция и Германия. При этом в июне 2020 года японский *Fugaku* (415,5 петафлопс) опередил американский *Summit* (Ок-Риджская национальная лаборатория) с мощностью в 148,6 петафлопс [48] и занял первое место. А ближайшим китайским конкурентом стал занявший 4 место *Sunway TaihuLight* (Национальный суперкомпьютерный центр, Уси). Лидерство *Fugaku* особенно важно в связи с использованием архитектуры ARM, а не x86, как у подавляющего большинства участников рейтинга.

Россия занимает 19 место (из 28) и представлена двумя суперкомпьютерами, лучший из которых *Кристофари*, созданный дочерней компанией Сбербанка с названием SberCloud в сотрудничестве с NVIDIA. Производительность данного суперкомпьютера составляет около 6,7 петафлопс, и соответствует условному 29-му месту в мире. В рейтинге отсутствуют отечественные суперкомпьютеры военного назначения. При этом вне всяких сомнений перед отечественным ядерным оружейным комплексом стоят задачи, аналогичные тем, которые решаются американскими коллегами в национальных лабораториях. Отметим, что именно ФГУП «РФЯЦ-ВНИИЭФ» (г. Саров), входящее в состав Государственной корпорации «Росатом», позиционирует себя как лидера «в области суперкомпьютерных технологий»[49].

В рамках СНГ существует и «внутренний» рейтинг «Топ-50» самых мощных компьютеров, который показывает, что и в нашей стране суперкомпьютерные технологии применяются как в науке, так и в бизнесе, хотя исследовательские задачи доминируют. При этом все суперкомпьютеры в рейтинге используют процессоры *Intel*[50].

В сентябре 2020 года в рамках реализации проекта Сибирского национального центра высокопроизводительных вычислений, обработки и хранения данных было подписано соглашение о создании сети суперкомпьютерных центров, целевой задачей которых является вхождение в топ-50 суперкомпьютеров в мире[51].

3.2. Суперкомпьютеры с ядерной родословной

На базе РФЯЦ-ВНИИЭФ с 2009 года реализуются основные проекты в ядерной сфере, причем 2020 год заявлен как срок достижения целевых показателей. Характеристики и особенности применения суперкомпьютеров непосредственно в г. Саров в открытой печати публикуются нерегулярно. В феврале 2012 года заявлялось, что суперкомпьютер РФЯЦ-ВНИИЭФ с производительностью свыше 1 петафлопса входит в десятку мощнейших в мире. Также указывались планы

[47] LIST STATISTICS // Веб-сайт Linpack Top-500. URL: https://www.top500.org/statistics/list/.

[48] Japan Captures TOP500 Crown with Arm-Powered Supercomputer // Веб-сайт Linpack Top-500. URL: https://www.top500.org/news/japan-captures-top500-crown-arm-powered-supercomputer/

[49] Костюков В.Е. Предложения по развитию российских суперкомпьютерных и информационных технологий. Проекты ФГУП «РФЯЦ-ВНИИЭФ» (Госкорпорация «Росатом»). Презентация на совещании под председательством Д.А. Медведева, 19.02.2016. URL: http://static.government.ru/media/files/p5s9xN7FOBTZFoMahAzjAGjSh0aiXBAJ.pdf.

[50] Научно-исследовательский вычислительный центр МГУ имени М.В. Ломоносова и Межведомственный Суперкомпьютерный Центр РАН объявляют о выпуске тридцать второй редакции списка Top50 самых мощных компьютеров СНГ // НИВЦ МГУ имени М.В. Ломоносова. 2020. 31 марта. URL: http://top50.supercomputers.ru/newsfeed_local/11.

[51] Сеть суперкомпьютерных центров создадут в Томске и Новосибирске // ТАСС. 2020. 16 сентября. URL: https://tass.ru/sibir-news/9468063.

доведения мощности до 5-10 петафлопс «в ближайшее время», а к сегодняшнему дню (2019-2020 годы) должна была быть реализована задача по переходу на уровень экзафлопса. Очевидно, что во всем мире существуют проблемы с выходом на такие характеристики. Вместе с тем в тематическом интервью в конце 2019 года данные о фактической производительности саровских суперкомпьютеров озвучены не были[52]. При этом в 2017 году ряд сотрудников РФЯЦ-ВНИИЭФ были уличены в майнинге криптовалюты[53]. Отметим, что еще в начале 2010-х годов РФЯЦ-ВНИИЭФ разработал линейку универсальных и специализированных компактных супер-ЭВМ с диапазонами производительности от 1 до 8 терафлопс[54]. Эти машины используются на предприятиях авиационно-космической и атомной отраслей. По состоянию на 2013 год сообщалось о поставке более 60 таких ЭВМ в различные организации[55]. Ярким свидетельством как минимум, позиционирования РФЯЦ-ВНИИЭФ в качестве лидера суперкомпьютерного направления в России, является предложение «Росатома» определить данную организацию единственным поставщиком систем суперкомпьютерного моделирования для ведомств и госкомпаний с 2020 по 2024 год, а именно – системы автоматизированного проектирования «Логос» [56]. На примере результатов деятельности РФЯЦ-ВНИИЭФ, а именно одного из патентов, зарегистрированных в 2018 году, можно оценить сложность обеспечения работы суперкомпьютеров как таковых, в первую очередь в части охлаждения вычислительных систем[57].

Смежники-ядерщики из РФЯЦ-ВНИИТФ в сотрудничестве с холдингом «Росэлектроника» (Научно-исследовательский центр электронной вычислительной техники концерна «Вега») в 2019 году создали вычислительный комплекс информационно-телекоммуникационного центра Военного инновационного технополиса «ЭРА» в Анапе [58]. Характеристики данного суперкомпьютера не публиковались, однако репортаж в ведомственном издании упоминает еще одну разработку «Росэлектроники» – «компактный мобильный суперкомпьютер» [59]. Как заявлялось в конце 2018 года, он способен к пиковой производительности в 2,2 петафлопс [60]. Отметим, что американский Военно-морской суперкомпьютерный центр (Navy DSRC) в настоящее время обладает примерно такой же мощностью[61]. Однако, уже к концу 2020 – началу 2021 годов ВМС США планируют принять в эксплуатацию новый суперкомпьютер с производительностью в 12,8 петафлопс,

---

[52] Российские суперЭВМ теряют позиции в «Топе-500». Это важно? // «Страна-Росатом». 2019. 24 сентября. URL: http://strana-rosatom.ru/2019/09/24/%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D0%BA%D0%B0-%D1%81%D0%BA%D0%BE%D1%80%D0%BE%D1%81%D1%82%D0%B8/.

[53] Биткойнам утроили майнинг в Сарове // Коммерсантъ. 2019. 26 октября. URL: https://www.kommersant.ru/doc/4140085.

[54] Компактные супер-ЭВМ // Веб-сайт ВНИИЭФ. URL: http://vniief.ru/unvisible_aria/products/it/razr/7e6f3b8049bdd12cbafefe3d902053fb.

[55] В Сарове федеральным ядерным центром изготовлено более 60 суперкомпьютеров // ТАСС. 2013. 30 июля. URL: https://tass.ru/ekonomika/554776.

56 «Росатом» грузится в суперкомпьютеры // Коммерсантъ. 2020. 31 августа. С. 5.

[57] Корзаков Ю. Н. и др. Система охлаждения массивно-параллельных вычислительных систем. 10.05.2018, Патент РФ 2653499.

[58] Ростех создал вычислительный комплекс для технополиса «Эра» // ГК «Ростех». 2019. 25 марта. URL: https://rostec.ru/news/rostekh-sozdal-vychislitelnyy-kompleks-dlya-tekhnopolisa-era/.

[59] Новая «ЭРА»: суперЭВМ, электронный супермозг // Еженедельник «Звезда». 2019. 29 марта. URL: https://zvezdaweekly.ru/news/t/20193281328-FqxE6.html.

[60] Ростех создал мобильный суперкомпьютер // Официальный веб-сайт ГК «Ростех». 2018. 23 ноября. URL: https://rostec.ru/media/pressrelease/rostekh-sozdal-mobilnyy-superkompyuter/.

[61] Navy DSRC // Веб-сайт Linpack Top-500. URL: https://www.top500.org/site/50425.

который станет мощнейшим во всем американском военном ведомстве [62] . В технополисе «ЭРА» предполагается, что введенная в эксплуатацию весной 2019 года супер-ЭВМ является лишь первым этапом, а в дальнейшем планируется наращивать вычислительные мощности. При этом, по данным СМИ, в мае того же года в этой организации сменился руководитель, что могло быть связано с конфликтом вокруг закупки суперкомпьютеров.[63] В рамках МВТФ «Армия-2020» было предварительно согласовано использование супер-ЭВМ технополиса «ЭРА» в работах над нейронными сетями глубокого обучения[64].

Отметим еще одну разработку «Ростеха» – первый суперкомпьютер на базе отечественных процессоров. В 2019 году ИНЭУМ им. И.С. Брука на российских 8-ядерных микропроцессорах «Эльбрус-8С» создана супер-ЭВМ с относительно скромной мощностью в 75 терафлопс. Однако в настоящее время сложно говорить о том, насколько распространенным окажется такое импортозамещение.

«Компактная Супер-ЭВМ» под индексом «АПК-1М3» с 2018 года применяется в 12-м ЦНИИ Минобороны России, к задачам которого относится «обоснование направлений развития и поддержания высокой боевой готовности и эффективности ядерных вооружений всех видов Вооруженных сил и родов войск РФ»[65]. АПК-1М3 обладает, казалось бы, не очень впечатляющей пиковой производительностью в 1,2 терафлопс, и используется для «проведения численного и имитационного моделирования реализации параллельных алгоритмов обработки большого объема информации при проведении научных исследований с последующей визуализацией расчетных данных»[66].

3.3. Применение суперкомпьютеров

Среди конкретных задач, решаемых с использованием супер-ЭВМ, разработанной 12-м ЦНИИ Минобороны России, указывается моделирование ряда явлений, в том числе:

- воздействия воздушной ударной волны на различные образцы вооружений и военной техники (в т.ч. на мобильные пусковые установки ракетных комплексов);
- «падения изделия на бетонную поверхность», под которым, исходя из иллюстраций, понимается оценка проникающей способности крылатых ракет с одной стороны и устойчивость защитных конструкций к поражению высокоточным оружием – с другой;
- воздействия электромагнитного излучения на приборный отсек, что является важным элементом оценки устойчивости тех или иных изделий к поражающим факторам ядерного взрыва – в первую очередь головных частей ракетных комплексов различных типов.

Прочие суперкомпьютеры (например, «Ломоносов» в МГУ, некогда бывший мощнейшим в России) используются для решения широкого диапазона задач в

---

[62] DoD to Install Cray-AMD System at Navy DSRC in Mississippi // Веб-сайт HPCWire. 2020. 17 февраля. URL: https://www.hpcwire.com/off-the-wire/dod-to-install-cray-amd-system-at-navy-dsrc-in-mississippi/.

[63] Начальник военного технополиса «Эра» перешел в администрацию президента // РБК. 2019. 27 мая. URL: https://www.rbc.ru/society/27/05/2019/5ce674799a794703564069ec.

64 Суперкомпьютер Военного инновационного технополиса «ЭРА» протестирует лучшие процессоры для нейронных сетей глубокого обучения // Официальный веб-сайт Минобороны России. URL: http://mil.ru/era/news/more.htm?id=12310458@egNews.

[65] Двенадцатый центральный научно-исследовательский институт Министерства обороны Российской Федерации имени В.А. Болятко (12 ЦНИИ МО) // Официальный веб-сайт Минобороны России. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=12994@morfDictionary.

[66] По информации, полученной автором на стенде 12 ЦНИИ в рамках МВТФ «Армия-2020».

области аэрокосмических технологий, создания лекарственных препаратов, сейсмологии и т.д. [67] Одним из примеров непосредственного использования суперкомпьютеров в целях, напрямую связанных с актуальными задачами обеспечения обороноспособности России, является выполнение расчетов в интересах разработки гиперзвуковых летательных аппаратов. Так, на базе инфраструктуры Межведомственного суперкомпьютерного центра Российской академии наук (МСЦ РАН) было выполнено моделирование высокоскоростных турбулентных течений на воздухозаборном устройстве [68] . Подобные задачи являются одним из ключевых элементов проектирования крылатых ракет с гиперзвуковыми прямоточными воздушно-реактивными двигателями.

В области космической техники использование суперкомпьютеров позволяет, например, осуществлять высокоточное имитационное моделирование нештатных ситуаций при посадке спускаемых космических аппаратов, учитывая все возможные сценарии и условия воздействия различных сред. Тем самым достигается сокращение сроков разработки, а также затрат на экспериментальную отработку тех или иных решений. Моделирование с применением суперкомпьютеров также позволяет получать более точные картину процессов турбулентности, что крайне важно для разработки в том числе двигателей и высокоскоростных систем[69].

В ноябре 2019 года в ЦНИИточмаш был запущен «программно-технологический комплекс «Центр» с производительностью в 50 терафлопс для моделирования испытаний стрелкового оружия и боеприпасов (оценки кучности стрельбы путем варьирования геометрических параметров и начальной скорости пули, условиями ее вылета из канала ствола)[70]. «Собственный» суперкомпьютер «Минин» пиковой производительностью в 57,6 терафлопс с 2012 года работает и в АО «ЦНИИ «Буревестник», одном из ведущих отечественных разработчиков артиллерийского вооружения. Интересно, что данное предприятие предоставляет вычислительные ресурсы суперкомпьютера в том числе и для внешних пользователей[71].

Мощности американского *Navy DSRC* используются для моделирования климата, погоды и мирового океана в интересах метеорологических подразделений ВМС США, что позволяет последовательно повышать прогнозы погоды и, как следствие, увеличивать эффективность применения сил и средств, обладая более точной картиной по сравнению с той, что имеется у противника.

Применяются суперкомпьютеры и в борьбе с пандемией SARS-CoV-2[72]. В частности, в США военные суперкомпьютеры используются для решения задач по повышению безопасности транспортировки зараженных с помощью воздушного транспорта и снижению рисков заражения для экипажей путем моделирования

---

[67] Суперкомпьютер «Ломоносов» // Официальный веб-сайт МГУ. URL: https://www.msu.ru/lomonosov/science/computer.html.

[68] Бендерский Л.А., Любимов Д. А., Рыбаков А.А. Анализ эффективности масштабирования при расчетах высокоскоростных турбулентных течений на суперкомпьютере RANS/ILES методом высокого разрешения // Труды научно-исследовательского института системных исследований Российской академии наук. – 2017. – Т. 7. – №. 4. – С. 32-40.

[69] Суперкомпьютерные технологии в науке, образовании и промышленности / Под ред. В.А. Садовничего, Г.И. Савина, В.В. Воеводина. - Сер. 7 Суперкомпьютерное образование – М.: МГТУ им. М.Ф. Ломоносова, 2017.

[70] Ростех ввел в строй суперкомпьютер «Центр» // Официальный веб-сайт ГК «Ростех». 2019. 8 ноября. URL: https://rostec.ru/news/rostekh-vvel-v-stroy-superkompyuter-tsentr-/.

[71] Центр высокопроизводительных вычислений в АО «ЦНИИ «Буревестник». URL: https://www.burevestnik.com/products/yslugi_c.html

[72] Pentagon Supercomputers Puzzle Out How to Safely Airlift Coronavirus Patients // Defense One. 2020. 13 апреля. URL: https://www.defenseone.com/technology/2020/04/pentagon-supercomputers-puzzle-out-how-safely-airlift-coronavirus-patients/164553/.

потоков воздуха и влаги внутри воздушных судов. Кроме того, вычислительные мощности суперкомпьютеров применяются для предварительной оценки эффективности потенциальных вакцин. Суперкомпьютер Ок-Риджской национальной лаборатории *Summit* был использован для генетических исследований больных новым коронавирусом, что позволило выявить конкретные процессы, собственно, болезни, вызываемой SARS-CoV-2 и, в перспективе, повысить эффективность лечения и разработки новых препаратов[73].

Следующем этапом развития, как уже упоминалось, станет переход на экзамасштаб, т.е. есть к супер-ЭВМ эксафлопсного уровня. Как заявляется, уже в самом ближайшем времени в США будут запущены два суперкомпьютера с мощность в более чем полтора эксафлопса каждый[74]. Стоимость их пятилетней разработки составила $1,8 млрд. США. В настоящее время более двух десятков команд ученых завершают подготовку задач, решение которых потребует такой мощности. К наиболее перспективным направлениям относят энергетическую отрасль, причем едва ли не все ее направления – от миниатюризации двигателей внутреннего сгорания до повышения эффективности ветровой энергетики. Новый импульс могут получить и работы в области термоядерной энергетики.

Все задачи, решаемые с применением суперкомпьютеров, условно можно отнести к высокоточному моделированию искусственных и естественных процессов (рисунок 3.2).

3.4. «Суперкомпьютерная» безопасность

Представляется обоснованным введение термина ***«суперкомпьютерная» безопасность***, под которым предлагается понимать *использование суперкомпьютерных технологий в интересах решения задач, связанных с национальной обороной в самом широком смысле*. *Безопасность при этом определяется как состояние защищенности жизненно важных интересов государства от внутренних и внешних угроз, исходящих из возможного кардинального преимущества других стран, а также негосударственных акторов в области суперкомпьютеров.*

В целом в рассматриваемой области суперкомпьютеры применяются в следующих ключевых областях:

- поддержание и модернизация ядерного арсенала в условиях отсутствия натурных экспериментов;
- оптимизация процессов разработки передовых видов вооружения и военной техники путем сокращения количества испытаний, благодаря качественно новым возможностям в области моделирования;
- метеорологические задачи в глобальном масштабе в интересах вооруженных сил для прогнозирования состояния различных сред и планирования операций с учетом всех необходимых внешних факторов.

В условиях обостряющейся конкуренции на мировой арене, соперничества «великих держав», а также учитывая, что ряд задач, для решения которых требуются суперкомпьютерные мощности, относятся к наиболее чувствительным

73 Anderson M. Has the Summit Supercomputer Cracked COVID's Code? // IEEE Spectrum. 2020. 2 августа. URL: https://spectrum.ieee.org/the-human-os/computing/hardware/has-the-summit-supercomputer-cracked-the-covid-code.

74 CLEANER-BURNING GASOLINE ENGINES, CITIES POWERED BY WIND, NUCLEAR REACTORS THAT FIT ON A TABLETOP—SOON THEY COULD ALL BE WITHIN REACH // Exascale Computing Project. 2020. 18 мая. URL: https://www.exascaleproject.org/cleaner-burning-gasoline-engines-cities-powered-by-wind-nuclear-reactors-that-fit-on-a-tabletop-soon-they-could-all-be-within-reach/.

отраслям науки и промышленности, прямо влияющим на обороноспособность, сложно надеяться на создание условий для расширения международного научно-технологического сотрудничества в данной сфере.

В настоящее время Россия уступает лидерам «суперкомпьютерной гонки» и качественно, и количественно. Вместе с тем нельзя сказать, что наша страна стоит на месте. Важную роль играет и объединение усилий различных участников отечественного «суперкомпьютерного рынка», обладающих соответствующими компетенциями. В связи с этим, как представляется, единственным путем сохранения и наращивания потенциала Российской Федерации в данной области является продолжение работы по созданию собственных суперкомпьютеров как на импортной, так и на отечественной элементной базе. Признанием важности этого направления стало проведение тематического круглого стола «Использование суперкомпьютерных технологий в Министерстве обороны Российской Федерации» в рамках МВТФ «Армия-2020» [75] , полной информации о котором, а также о представленных оценках и предложениях до настоящего времени в открытых источниках не появилось.

Рисунок 3.2. Области применения суперкомпьютеров

Источник: рисунок построен автором.

Значительным подспорьем для повышения точности оценок в данной области могло бы стать участие отечественных суперкомпьютеров оборонного назначения во

[75] Использование суперкомпьютерных технологий в Министерстве обороны Российской Федерации // Официальный веб-сайт МВТФ «Армия». URL: https://www.rusarmyexpo.ru/business_program/4107/33388.html.

внутренних рейтингах. Подобный подход, помимо очевидной пользы для экспертного сообщества и исследовательских организаций, способствовал бы улучшению имиджа России в качестве одной из стран-флагманов глобальной цифровой трансформации. Кроме того, не исключено, что в рамках процессов диверсификации оборонно-промышленного комплекса, большая открытость информации о вычислительных мощностях различных предприятий и доступ к этим мощностям со стороны коммерческих пользователей могли бы способствовать росту доли «гражданской» выручки предприятий оборонной отрасли.

ГЛАВА 4.

Стратегическая стабильность и информационно-коммуникационные инновации

4.1. Стратегическая стабильность в эру информационно-коммуникационных технологий

Под термином «*стабильность*» в любой области понимают устойчивость, постоянство или способность системы функционировать, сохраняя неизменной свою структуру и возвращаться в состояние равновесия даже после воздействия дестабилизирующих сил (факторов). В военно-политической сфере принято считать, что чем выше уровень стратегической стабильности, тем меньше вероятность широкомасштабной, и, в первую очередь, ядерной войны. В отношениях между ядерными державами понятие «*стратегическая стабильность*» в течение многих лет определялась как *состояние их взаимоотношений, при котором устраняются стимулы к нанесению первого ядерного удара*. Основой тому служило осознание того факта, что в обеспечении необходимого и достаточного уровня стратегической стабильности были заинтересованы все страны мира, но наибольшую ответственность несли две крупнейшие ядерные державы. Поскольку ядерное оружие по-прежнему существует и его разрушительные возможности постоянно совершенствуются, сегодня это понимание стратегической стабильности так же актуально, как и в период холодной войны, когда оно формировалось.

Однако за последние три десятилетия ситуация существенно изменилась, представления о способах и механизмах предотвращения ядерной войны, выработанные в период биполярности, уже не в полной мере соответствуют сегодняшним геополитическим реалиям и уровню развития технологий. Эти значительные изменения в международных военно-политических отношениях требуют учета не только ядерной составляющей, но и другие показатели, сохраняя при этом традиционную суть. Кроме того, сегодня речь идет уже не о двух глобальных полюсах противостояния, как во время биполярности, а об увеличении количества субъектов, влияющих на уровень стратегической стабильности. Следовательно, сегодня необходимо говорить не о полюсах, а о системе, а значит, оценивать возможности и характеристики *современной военно-политической системы*.

Рассматривая *стратегическую стабильность военно-политической системы* как *состояние мира (отсутствие широкомасштабной войны) в рамках этой системы, которое поддерживается даже при постоянно действующих возмущениях (дестабилизирующих факторах) в течение определенного (заданного) периода времени*[76], в настоящее время можно констатировать наличие нескольких глобальных проблем, связанных с отсутствием общего для мировых держав понимания основных участников процесса обеспечения стратегической стабильности, характеристик военно-политической системы, которые должны сохраняться в течение запланированного времени, и самое главное – дестабилизирующих факторов.

Следовательно, на профессиональном уровне необходимо говорить не просто о «поддержании» стратегической стабильности, о «сохранении» стратегической

[76] Ромашкина Н.П. Стратегическая стабильность в современной системе международных отношений. – М.: Наука, 2008. URL: http://www.avnrf.ru/index.php/drugie-publikatsii/590-strategicheskaya-stabilnost-v-sovremennoj-sisteme-mezhdunarodnykh-otnoshenij.

стабильности, о ее «укреплении» и т.д., а о необходимости *обеспечения* стратегической стабильности, выработки новых общих качественных и, что особенно важно, количественных подходов к оценке ее уровня на базе имеющегося опыта. А для этого необходимо договариваться об общих критериях оценки.

Процесс обсуждения таких критериев был остановлен на двустороннем уровне РФ-США с середины 1990-х годов, так как Соединенные Штаты не считали это нужным. Сегодня это привело к глобальной проблеме, потому что снижение уровня стратегической стабильности ниже необходимого и достаточного крайне опасно для всех без исключения государств. Следовательно, в обеспечении необходимого и достаточного уровня, как и ранее, заинтересованы все страны мира, и, по-прежнему, наибольшую ответственность несут государства-обладатели ЯО, количество и роль которых изменились.

Каковы же характеристики системы, в которой жизненно важно обеспечивать необходимый и достаточный уровень стабильности, какие новые дестабилизирующие факторы возникли за последние десятилетия?

1. *Изменение показателей системы международных отношений после периодов биполярности и монополярности во главе с США* в условиях осложнения военно-стратегических отношений России и США, а также с появлением нового глобального центра силы — Китая, который не вовлечен в процесс ядерного разоружения.

2. *Постепенное разрушение режима ограничения и сокращения стратегических вооружений* после выхода США из Договора об ограничении систем противоракетной обороны (ПРО) и Договора о ликвидации ракет средней и меньшей дальности (РСМД), при неустойчивом существовании межгосударственных договоренностей по обычным вооружениям и в условиях отсутствия официальных переговоров по ограничению и сокращению ядерных вооружений на исходе действия Договора СНВ-3.

3. *Ракетно-ядерная многополярность*, которая выражается в увеличении количества государств с ракетными и ядерными вооружениями, а также с ростом вероятности дальнейшего их распространения (таблица 4.1).

4. *Доктринальные изменения в ядерных государствах*, которые формально призваны укрепить сдерживание, а фактически снижают порог применения ядерного оружия.

5. *Эволюция военных доктрин и стратегий государств-членов НАТО, их союзников и партнеров в сфере ИКТ*, допускающих применение оборонительных мер в ответ на ИКТ-атаку как в военное, так и в мирное время. Принципиальное значение имеет решение НАТО о применении Статьи 5 Устава Альянса в ответ на кибернападения.

6. *Создание широкомасштабной системы ПРО США* (рисунок 4.1).

7. *Возрастание роли и мощи неядерных (высокоточных и высокоинтеллектуальных) видов оружия в стратегическом планировании*.

8. *Базирование на одних и тех же платформах ядерных и неядерных вооружений*, в результате чего пуск баллистических или крылатых ракет с обычным вооружением может рассматриваться оппонентом как применение ядерного оружия.

9. *Появление ядерных вооружений малой мощности*, наличие которых снижает порог применения ЯО и повышает вероятность перерастания вооруженного конфликта в ядерную войну.

10. *Развитие новейших противоспутниковых средств на основе ИКТ*, позволяющих уничтожать спутники при помощи размещенных на земле противоспутниковых систем, а также влиять на работу не только искусственных спутников Земли мирного, но также двойного и военного назначения, включая

элементы систем предупреждения о ракетном нападении (СПРН)[77]. Такие средства могут повлиять на эффективность работы спутников в рамках систем Ведения боевых действий в едином информационном пространстве, которые активно совершенствуются в развитых в военном отношении государствах. Это одна из самых серьезных угроз стратегической стабильности на современном этапе. Напомним, что в июне 2018 года впервые была озвучена информация о кибервмешательстве в работу американского спутника военного назначения, когда, по утверждению компании *Symantec*, внедрение «закладки» в ПО СУ позволило изменить орбиту спутника и перехватить чувствительные данные[78].

Таблица 4.1. Государства, обладающие баллистическими ракетами

№	Государство	№	Государство	№	Государство
1	Азербайджан	**14**	Греция	**27**	ОАЭ
2	Алжир	**15**	Дания	**28**	Пакистан
3	Ангола	**16**	Израиль	**29**	Республика Корея
4	Аргентина	**17**	Индия	**30**	РФ
5	Армения	**18**	Ирак	**31**	Сербия и Черногория
6	Афганистан	**19**	ИРИ	**32**	Сирия
7	Бахрейн	**20**	Йемен	**33**	США
8	Белоруссия	**21**	Казахстан	**34**	Тайвань
9	Бразилия	**22**	КНДР	**35**	Туркменистан
10	Великобритания	**23**	КНР	**36**	Турция
11	Вьетнам	**24**	Куба	**37**	Украина
12	Египет	**25**	КСА	**38**	Франция
13	Германия	**26**	Ливия	**39**	Япония

Источник: таблица построена автором.

11. *Возможность милитаризации космического пространства, в том числе с использованием новейших ИКТ.*

12. Помимо технологических характеристик, влияющих на уровень стратегической стабильности, сегодня все больше экспертов из разных стран обращают внимание на еще одну особенность современного мира – психологическую. Ее можно сформулировать как *утрату страха перед ядерной войной у общества и политических элит* [79]. Такое положение дел может существенно снизить порог применения вооружений, в том числе ядерных.

[77] По последним данным, в космосе находится более двух тысяч действующих спутников: более 900 принадлежат США, около 150 – России, около 300 – Китаю и остальные – другим государствам.

[78] Symantec зафиксировала кибератаку на компании-операторы спутников в США и Азии // ТАСС. 2018. 20 июня. URL: https://tass.ru/mezhdunarodnaya-panorama/5306217.

[79] Тренин Д. В. Стратегическая стабильность в условиях смены миропорядка // РСМД. 2019. 20 марта. URL: https://russiancouncil.ru/analytics-and-comments/comments/strategicheskaya-stabilnost-v-usloviyakh-smeny-miroporyadka/.

Рисунок 4.1. Государства – союзники и партнеры США по созданию широкомасштабной системы ПРО

Источник: рисунок построен автором.

При разработке критериев оценки уровня стратегической стабильности и основанных на этом конкретных планов по ее обеспечению целесообразно учитывать как общие для любого исторического периода характеристики, так и особенности современного этапа. Ускоренное развитие информационно-коммуникационных технологий в настоящее время является одной из таких исключительных особенностей. При этом все дестабилизирующие факторы сегодня усугубляется возможностью использования ИКТ в деструктивных целях. Отсутствие глобальных механизмов управления в этой сфере (см. главу 1 монографии) также ведет к снижению уровня стратегической стабильности по сравнению с периодом биполярности. Киберугрозы обостряют, осложняют, углубляют, усиливают и видоизменяют те проблемы, которые всегда существовали в обеспечении безопасности ЯО (рисунок 4.2).

Можно выделить несколько глобальных проблем стратегической стабильности, исходящих из информационного пространства.

Проблема 1. Р*ост вероятности выведения из строя или уничтожения ЯО посредством вредоносного воздействия ИКТ, что уже сегодня влияет на перспективы ядерного разоружения и нераспространения*. С одной стороны, появление такой возможности может стать для государств-обладателей ЯО поводом для ускоренного сокращения своих вооружений. А с другой стороны, что более вероятно, может послужить серьезной причиной для масштабной модернизации ЯО, создания более сложных и защищенных систем, что приведет к качественной и (или) количественной гонке ядерных вооружений и как следствие – к снижению уровня стратегической стабильности. Кроме того, вопросы информационной безопасности уже влияют не только на перспективы ядерного разоружения и нераспространения, но и на существующие ограничительные режимы.

Рисунок 4.2. Стратегические ядерные вооружения: некоторые ИКТ-уязвимости и потенциальные последствия

Примечание: информационно-ударная техносфера – совокупность технических информационных, управляющих, ударных, обеспечивающих и обслуживающих устройств и систем вместе с областью военно-технической деятельности человека.

Источник: Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. – 2019. № 1. URL: https://cyberrus.com/wp-content/uploads/2019/03/02-09-129-19_1.-Romashkina.pdf.

Проблема 2. Самая серьезная, хотя пока и маловероятная угроза – *влияние ложной информации, полученной от ИКТ, на вероятность ошибочного санкционированного пуска баллистических ракет (БР), а также на принятие решения о применении ЯО*. Задача защиты БР от ошибочных пусков возникла с момента создания первых ракет. Она всякий раз решается заново при создании новых БР, постановке их на дежурство, при подготовке и проведении испытательных, учебно-боевых и контрольно-боевых пусков. Несмотря на то, что и США, и Россия (СССР) всегда уделяли этому большое внимание, за десятилетия существования ЯО в обеих странах были случаи технических сбоев и человеческих ошибок, которые могли бы спровоцировать ядерный пуск. Уменьшение вероятности ошибочного пуска, которая никогда не равна нулю, будет стоять более остро по мере перехода войск стратегического назначения на цифровые технологии передачи информации. Так, по данным Министерства обороны России, наши Ракетные войска стратегического назначения (РВСН) должны полностью перейти на цифровые технологии в 2020 году[80].

[80] К 2020 году РВСН полностью перейдут на цифровые технологии передачи информации // Сайт Министерства обороны Российской Федерации URL: https://structure.mil.ru/structure/forces/strategic_rocket/news/more.htm?id=12142122%40egNews.

Эта проблема связана со следующими возможностями ИКТ:

- получение ложной информации от систем предупреждения о ракетном нападении (СПРН) о запуске баллистических ракет с ЯО со стороны противника;
- внедрение в управление коммуникационными системами в командных пунктах РВСН для создания ситуации ошибочного санкционированного пуска;
- непосредственное внедрение в электронные системы связи, командования и контроля над ЯО (автоматизированные системы боевого управления – АСБУ – в российской терминологии, Nuclear Command, Control, and Communications – NC3 – в западной терминологии).

Во время хакерских нападений могут быть повреждены или разрушены каналы коммуникаций, созданы помехи в системе управления вооруженными, в том числе ядерными силами, а также снижена уверенность военных, принимающих решения, в работоспособности и эффективности систем управления, командования и контроля (КК ЯО на рисунке 4.4). Например, нападающие могут использовать DDoS-атаки для нарушения систем коммуникации, управления и целеполагания. В кризисной ситуации ИКТ-нападения могут негативно повлиять на принятие решения об ответных действиях. Угроза выведения из строя военных систем под воздействием ИКТ-средств может сократить поиск альтернатив военным действиям и создать значительные проблемы для успешной передачи сигналов. В результате «лестница эскалации» конфликта сократится, что, в свою очередь, может вызвать соблазн победить в войне без получения ответного удара (рисунки 4.3, 4.4).

Кроме того, эта проблема связана с возможностями использования так называемого «ложного флага» при кибервмешательстве, когда операции проводятся таким образом, чтобы создавалось впечатление, что они были выполнены другим субъектом. При этом также не исключена вероятность восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения. Все это повышает вероятность ошибочного запуска БР, а, следовательно, снижает уровень стратегической стабильности.

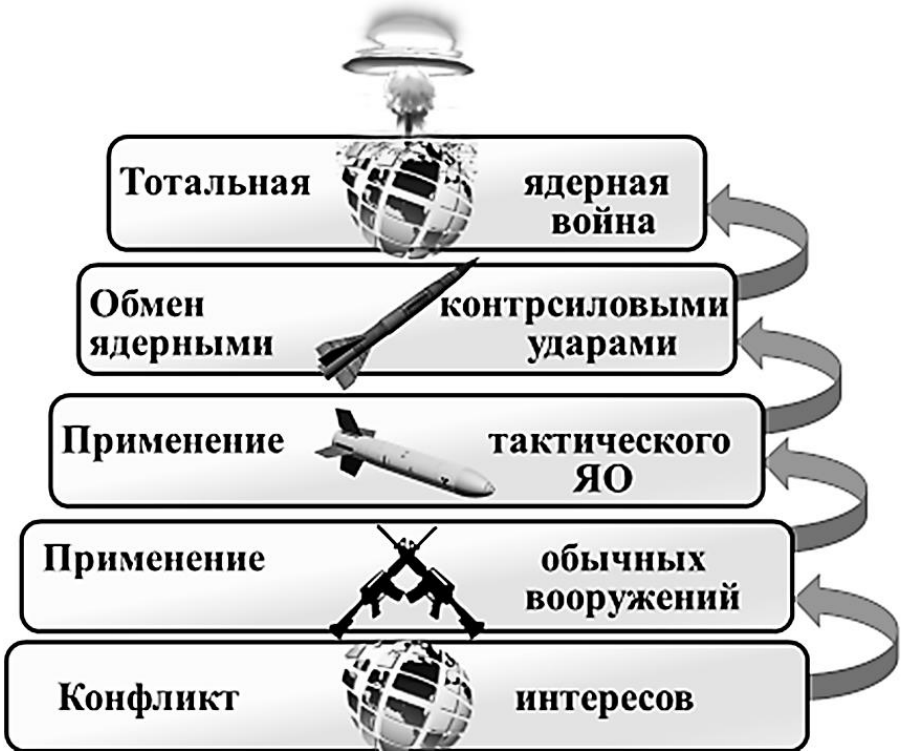
Угрозы дополнительно усиливаются в связи с развитием ударных роботизированных средств с дистанционным управлением [81] , искусственного интеллекта в военных целях, машинного обучения, возможностями автономной работы различных систем и подсистем, автоматизированных систем принятия решений и т.д., которые могут подвергаться ИКТ-атакам, средств кибер-электромагнитной деятельности, которую активно развивают в США и которая включает в себя кибероперации, электронную, войну, электронные атаки в мирное время, операции по управлению электромагнитным спектром, а также подавление целей активными и пассивными помехами и электромагнитная дезинформация[82].

[81] Балыбин В.А., Высторобский С.Г., Ельцов О.Н., Сырбу И.А. Роботизированные комплексы РЭБ: перспективы создания и применения. Радиоэлектронная борьба в Вооруженных Силах Российской Федерации – 2018. Материалы от войск радиоэлектронной борьбы ВС РФ. 2018. URL: https://reb.informost.ru/2018/pdf/1-5.pdf.

[82] Cyber Electromagnetic Activities. Field Manual No. 3-38 // Washington, Headquarters Department of the Army. 2014/ 12 февраля. URL: https://info.publicintelligence.net/USArmy-CEMA.pdf.

Горбачев Ю.Е. Радиоэлектронная борьба в сложной электромагнитной обстановке. Радиоэлектронная борьба в Вооруженных Силах Российской Федерации – 2017. Материалы от войск радиоэлектронной борьбы ВС РФ. 2017 URL: https://reb.informost.ru/2017/pdf/1-3.pdf.

Рисунок 4.3. «Лестница эскалации» ядерной войны



Источник: рисунок построен автором.

Рисунок 4.4. Лестница эскалации конфликта с применением ИКТ

Источник: рисунок построен автором.

Одна из современных возможностей снижения ИКТ-угроз в военной сфере – разработка квантовых криптографических систем для защиты информации, в том числе, оборонного характера. По данным министерства обороны РФ, у России тоже есть потенциал для производства таких систем, в том числе, военного назначения[83]. Отметим, что квантовая криптография – метод защиты коммуникаций, основанный на принципах квантовой физики в отличие от традиционной криптографии на основе математических методов. Процесс отправки и приёма информации в квантовой криптографии выполняется физическими средствами, например, при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи. Таким образом, обеспечивается постоянная и автоматическая смена ключей при передаче каждого сообщения в режиме одноразового «шифроблокнота». Технология опирается на принципиальную неопределённость поведения квантовой системы – невозможно измерить один параметр фотона, не исказив другой. Поэтому можно создать такую систему связи, которая всегда будет обнаруживать вмешательство: попытка измерения параметров в квантовой системе вносит в неё нарушения, разрушая или искажая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать, что действует перехватчик. На сегодняшний день это единственный вид шифрования со строго доказанной криптографической стойкостью.

Проблема 3. Роль ядерного оружия в предотвращении информационных нападений на военные и другие критически важные объекты инфраструктуры государств. Пока данная проблема выглядит сугубо теоретической. Но с учетом быстрого нарастания угроз в информационном пространстве, необходимо отдавать себе отчет в том, что ядерная и информационная сферы, видимо, будут еще более взаимосвязаны в будущем, и этот вопрос может встать более остро.

4.2. Информационно-коммуникационные технологии и ядерное сдерживание

В контексте стратегической стабильности важнейшими и вместе с тем недостаточно исследованными являются конкретные ИКТ-угрозы в отношении различных элементов систем эксплуатации и применения ядерного оружия, непосредственно самого ЯО, а также обеспечивающих контуров управления и связи, поэтому они требуют дополнительного экспертного анализа.

4.2.1. Направления и средства воздействия

В целях данного анализа под ***ИКТ-угрозами*** предлагается понимать *потенциальную возможность вмешательства в нормальное (запланированное) функционирование различных систем и подсистем управления ядерным оружием и его носителями (в том числе бортовых) с использованием кибернетических и иных информационных технологий («кибервоздействие»)* [84] . В общем виде направления и цели такого воздействия представлены на рисунке 4.5.

[83] Инфофорум-2018. Минобороны РФ обдумывают идею разработки квантовых криптомашин // Сайт «Национальный форум информационной безопасности «Инфофорум». URL: https://infoforum.ru/news/infoforum-2018-minoborony-rf-obdumyvaut-ideu-razrabotki-kvantovyh-kriptomashin.

[84] Определение автора.

Рисунок 4.5. Кибервоздействие и ядерное оружие

Источники: Стаутленд П., Питтс-Кифер С. Ядерное оружие в новую киберэпоху // Инициатива по сокращению ядерной угрозы (NTI). 2018 URL: https://media.nti.org/documents/Nuclear_Weapons_in_the_New_Cyber_Age-Russian_Translation.pdf; Ромашкина Н. Стратегическая нестабильность в эпоху ИКТ: кризис или новая норма? // РСМД, 2019. URL: https://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-nestabilnost-v-epokhu-ikt-krizis-ili-novaya-norma/.

Выделим несколько типов атак в рассматриваемой области на основе используемых средств и технологий:

1) вредоносное ПО, внедряемое через внешнюю сетевую инфраструктуру с использование сетей общего пользования или путем скрытного подключения к закрытым сетям;
2) вредоносное ПО, внедряемое с помощью физических носителей информации, как сознательно («своими агентами»), так и путем подмены устройств, используемых операторами тех или иных систем и подсистем;
3) средства радиоэлектронной борьбы (РЭБ) тактического и стратегического назначения различных видов базирования;
4) «закладки» в элементной и программной базе оборудования на этапе его создания и поставки на предприятия, осуществляющие производство и финальную сборку в интересах соответствующих заказчиков;
5) обман датчиков сбора информации всех типов, используемых в системе предупреждения о ракетном нападении, боевого управления, а также различных системах поддержки принятия управленческих решений.

Особенностью вредоносного ПО, применяемого, в том числе, в военных операциях (ИКТ-оружия, кибероружия), является невозможность достоверно определить цель противника, даже если само ПО уже обнаружено. Идентичные образцы ИКТ-оружия могут применяться как для сбора информации, так и для оказания кибервоздействия на системы, в которые они внедрились.

Другая особенность кибероружия, в определенной мере роднящей его с оружием ядерным, заключается в разделении носителя и полезной нагрузки: один и тот же продукт может использоваться для внедрения вредоносных программ как предназначенных для наблюдения и сбора информации, так и для перехвата управления оружейными комплексами либо вывода из строя командных сетей. Таким образом, возникает своего рода вилка в принятии решений как нападающей, так и обороняющейся сторонами: после успешной доставки относительно «безвредной» программной боевой части в сети обороняющегося при эскалации напряженности между сторонами возможна попытка замены «безвредной» БЧ на «ударную». При этом «обороняющийся» может своевременно обнаружить изначальную атаку и в условиях отсутствия достоверной информации о планах «нападающего» нанести собственный ответный или ответно-встречный удар, при этом уже не ограничивая себя киберпространством. Естественно, в данной ситуации речь идет о сетях, напрямую связанных с ядерным оружием и выживанием государства.

В связи с этим представляется целесообразным дополнительно детализировать классификацию по целям враждебного воздействия: сбор информации о противнике; «подмена» информации, используемой противником; вывод оборудования противника из строя; предотвращение применения ядерных сил противника; непреднамеренное применение противником его ядерных сил, прежде всего, против третьих стран. С учетом этой классификации можно оценить различные элементы видов ядерных сил с точки зрения их уязвимости.

Отдельно отметим, что можно выделить четыре основные категории субъектов, действующих на стыке ИКТ-пространства и ЯО: государства, их «прокси» (ассоциированные негосударственные организации), частные структуры (террористические и коммерческие) и так называемые «одинокие волки». Государства обладают наибольшим потенциалом, однако в контексте ядерного оружия они же являются наиболее уязвимыми, выступают главной потенциальной жертвой. Негосударственные субъекты, как правило, привлекаются к участию в межгосударственной борьбе. Частные структуры могут использовать кибероружие для шантажа ядерных держав либо предлагать свои услуги для обеспечения их обороноспособности. Одиночки могут пытаться монетизировать свои навыки путем их демонстрации наиболее ярким образом, либо руководствоваться идеологическими или эмоциональными мотивами. При этом подходы одного и того же субъекта к киберпространству и деятельности с использованием ИКТ (в том числе, условно-боевой) могут существенно различаться. Например, в части возможности использования посредников, демонстрации собственного потенциала, комментариев официальных лиц о фактах наступательных или оборонительных операций с применением ИКТ, а также подходов к оценке серьезности киберинцидентов и их расследованию.

4.2.2. Объекты ударов: центры управления

Как уже отмечалось, наиболее катастрофические последствия может вызвать вмешательство в системы управления ядерными силами, а также систему СПРН. Контуры управления отдельными элементами сил и средств ядерного сдерживания разделены, однако на определенном этапе все решения принимаются на уровне

высшего военно-политического руководства страны. Соответственно, от качества и своевременности информации, поступающей в центры принятия решений, а также от скорости и целостности доведения приказов до подразделений и боевых расчетов напрямую зависит эффективность реагирования на складывающуюся обстановку.

Серьезную угрозу представляет собой и использование средств РЭБ в целях «обмана» СПРН и средств ПРО.

Проблема уязвимости систем управления ЯО усугубляется высокой степенью готовности СЯС к применению. Теоретически сокрушительный «обезоруживающий» удар может быть нанесен с помощью кибероружия. При этом осознание риска кибератаки со стороны «вероятного противника» создает стимул к укреплению защиты сетей управления СЯС от актов незаконного вмешательства вне зависимости от их источников, что в целом способствует поддержанию стратегической стабильности. Аналогичная проблема может возникнуть и применительно к ракетным комплексам третьих ядерных держав. Для них ЯО является исключительной ценностью, и угроза его потери в случае нарушения каналов доведения команд является максимально серьезной. Во избежание сценария обезглавливающего кибердара возможно делегирование полномочий на применение ЯО нижестоящим уровням командования, что еще более усугубляет опасность: реакция на ложную тревогу, либо ложное понимание оперативной обстановки со стороны исполнителя может повлечь ядерную эскалацию, а рост количества уполномоченных командиров очевидным образом ведет к пропорциональному росту такой угрозы. Очевидно, атаки с использованием ИКТ существенно увеличивают подобные риски.

В сфере ИКТ-угроз и в целом влияния прорывных технологий на ЯО, вновь встает один из традиционно острых вопросов ядерного сдерживания: какая степень боеготовности является наиболее «стабилизирующей»? В случае России и США высокая степень готовности баллистических ракет межконтинентальной дальности к пуску остается оптимальным решением, так как гарантирует возмездие, удерживающее вероятного противника от первого удара. Таким образом, гарантия неизбежного возмездия перевешивает угрозу случайного пуска в глазах высшего военно-политического руководства двух стран. Вместе с тем, как Россия, так и США осуществляют значительные инвестиции в формирование максимально «живучего» потенциала ответного удара (в том числе «глубокого»).

Наличие кибероружия, боевые действия в цифровом пространстве, стремление государственных и негосударственных акторов получить преимущество над вероятным противником путем нанесения ущерба его ядерному оружию (концепция «предотвращения пуска»), либо создания условий его ошибочного применения – реальные факторы, которые необходимо учитывать.

4.2.3. Объекты ударов: боевые системы

ИКТ-угрозы присутствуют и на других эшелонах управления и боевого применения ядерных сил. Для оценки угроз представляется целесообразным учитывать следующие факторы:

- цифровизация элементной базы;
- связанность с иными элементами информационно-коммуникационной инфраструктуры вооруженных сил и за их пределами;
- степень боеготовности, в том числе в контексте наличия готовых к применению ядерных боезарядов непосредственно на носителях.

Попытка разделения непосредственно ядерных сил на несколько условных подгрупп представлена на рисунке 4.6.

Рисунок 4.6. Классификация ядерных сил

Источник: Энциклопедия РВСН // Официальный сайт Министерства обороны Российской Федерации. URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/listrvsn.htm.

Вмешательству могут быть подвержены как управляющие контуры на уровне подразделений, так и непосредственно пусковые установки, морские носители ракетного вооружения (в том числе подводные) и самолеты тактической и стратегической авиации, а также, собственно, боеприпасы и боезаряды. Конечно, здесь вряд ли можно говорить об «атаке первого типа» согласно классификации, представленной в первой части данного раздела, то есть через вредоносное ПО, внедряемое через внешнюю сетевую инфраструктуру с использование сетей общего пользования или путем скрытного подключения к закрытым сетям. Разве что в каком-то отдельном подразделении в нарушение всех возможных инструкций и

регламентов будет допущено сопряжение внутренних автоматизированных рабочих мест и систем управления с внешними сетями (что, все же, не исключено).

Однако агентурная подмена носителей информации («атака второго типа») вполне возможна. Такая угроза реальна в отношении подразделений ядерных сил всех типов базирования, хотя находящиеся на боевом патрулировании подводные крейсеры, воздушные ракетоносцы и подвижные грунтовые ракетные комплексы подвержены ей в меньшей мере.

Именно вышедшие из мест базирования и, соответственно, многослойной обороны от всех возможных видов воздействия со стороны противника носители становятся реальной целью для «атаки третьего типа» с использованием РЭБ. Современные средства РЭБ также могут оказывать направленное воздействие на информационно-коммуникационные системы противника с помощью формирования направленных помех. В этом случае главная угроза состоит в нарушении каналов связи, а также искажении информации, необходимой для целеуказания. Учитывая высокий уровень технологической сложности современных средств доставки ядерного оружия, не исключено, что воздействие с применением РЭБ может воспрепятствовать и непосредственно пускам ракетного оружия различного назначения путем радиоэлектронного поражения систем и средств управления оружием, а также разрушения, уничтожения или искажения программного обеспечения и информации в АСУ[85]. Очевидно, значительному радиоэлектронному воздействию на этапе выхода в позиционные районы и на рубежи пусков ракет могут быть подвержены носители тактического ядерного оружия независимо от вида базирования.

Проблема «закладок» как в «железе», так и в ПО является понятной и осознанной всеми причастными службами[86], что нашло отражение в весьма строгих подходах к лицензированию соответствующей продукции, используемой при производстве и постановке на боевое дежурство различных систем вооружения и военной техники. Вместе с тем никто не застрахован от ошибок, и здесь крайне важной задачей становится импортозамещение в самом прямом и жестком смысле этого слова. Достоверная информация о количестве иностранных комплектующих в различных носителях ядерного оружия и средствах его доставки отсутствует, однако можно предположить, что чем более массовым является изделие (особенно в случае наличия неядерных и экспортных версий), тем выше вероятность «атаки четвертого типа» в связи с ростом возможностей получения вероятным противником информации об архитектуре тех или иных систем вооружений.

Повсеместной стала ирония со стороны средств массовой информации и отдельных экспертов над низкотехнологичными носителями информации, применяемыми в области СЯС[87]. Вместе с тем, возможно, такой подход является одним из наиболее эффективных путей защиты критической военной инфраструктуры от кибератак. При этом для снижения киберугрозы целесообразно использовать исключительно национальное оборудование и ПО, максимально несовместимое с международными стандартами.

---

[85] Эволюция радиоэлектронной борьбы // Официальный сайт Государственной корпорации «Ростех». URL: https://rostec.ru/analytics/evolyutsiya-radioelektronnoy-borby/.

[86] ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования; ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

[87] The Pentagon’s Huge Atomic Floppies // Time. 2016. 25 мая 2016. URL: https://time.com/4348494/pentagon-nuclear-floppy-disks/.
Минобороны США пользуется старыми дискетами // ТК «Звезда». 2016. 27 мая. URL: https://tvzvezda.ru/news/vstrane_i_mire/content/201605270448-hoer.htm.

4.2.4. Фактор искусственного интеллекта

Все перечисленные выше угрозы дополнительно усиливаются в связи с развитием технологий искусственного интеллекта (ИИ), машинного обучения и возможностями автономной работы различных систем и подсистем.

Искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений; технологии искусственного интеллекта - технологии, основанные на использовании искусственного интеллекта, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта[88].

Машинное обучение (Machine Learning, ML) – это *раздел теории искусственного интеллекта, предметом которого является поиск методов решения задач путем обучения в процессе решения сходных задач. Для построения таких методов используются средства алгебры, математической статистики, дискретной математики, теории оптимизации, численных методов, и других разделов математики*[89].

СПРН является важнейшей областью для автономного анализа и подготовки решений. Основными задачами для технологий ИИ в этом случае являются оценка угрозы и прогноз ущерба, что может помочь разработать корректные сценарии ответных действий с учетом масштабов атаки, ее источника и возможных намерений. Машинное обучение и соответствующие технологии будут выполнять функцию поддержки принятия решений по мере перехода к ответным действиям, в частности, при организации маневрирования для вывода сил и средств из-под ударов противника, оптимизации планирования ответно-встречного удара. Слияние данных из различных источников и обновление информации в реальном масштабе времени способствуют повышению качества боевого управления и ситуационной осведомленности [90] . Однако именно по этой причине значительную угрозу представляет применение кибероружия: фактически, происходит умножение рисков, изложенных в данной главе.

Кроме того, существует угроза абсолютной подмены «человеческого» анализа оперативной обстановки из-за формирования оценок и решений военнослужащих исключительно на основе предложений автоматизированной системы. Фактически, человек присутствует в процедуре оценки ситуации, принятия решений и применения оружия, но все его решения принимаются под мощнейшим влиянием «машинных» данных. В такой ситуации возможен рост негативных последствий враждебного внешнего воздействия на информационные системы, обеспечивающие доведение исходных данных до автоматизированных средств поддержки принятия решений, а также систем, непосредственно осуществляющих подготовку этих решений.

---

[88] Национальная стратегия развития искусственного интеллекта на период до 2030 года, утверждена Указом Президента Российской Федерации от 10 октября 2019 г. № 490.

[89] Миронов А.М. Машинное обучение, часть 1. URL: http://www.intsys.msu.ru/staff/mironov/machine_learning_vol1.pdf.

[90] Руководство по многосенсорному слиянию данных: теория и практика / Под ред. М. Лиггинс, Д. Холл, Дж. Ллинас (2-е изд.). – Тэйлор&Фрэнсис, 2009.

Эффективным направлением использования машинного обучения, технического зрения и подобных технологий для бортовых подсистем средств доставки ЯО в настоящий момент представляется целеуказание. С помощью автоматизированной обработки и анализа изображений возможны оперативное и эффективное распознавание видов целей, уточнение их местоположения, наличие уязвимостей – а в конечном итоге и оптимизация количества используемых боезарядов[91]. ИИ в бортовых системах управления обеспечит высокую точность и маневрирование, непредсказуемое для оборонительных систем. Например, гиперзвуковые планирующие крылатые боевые блоки испытывают понятные сложности с внешним управлением в ходе полета в связи со скоростями и образованием облака плазмы – что приводит к необходимости поиска эффективных бортовых решений. Преодоление ПРО также может быть более эффективным с применением «умных» ложных целей и случайными изменениями траектории полета. При этом гонка в сложности между обороняющейся и наступающей сторонами будет вестись бесконечно, и кибервоздействие, РЭБ или иные способы некинетического перехвата путем обмана «умной» боеголовки, вероятно, также разрабатываются. Напомним, что первая битва средств РЭБ в области, непосредственной связанной с ЯО, произошла еще на заре «атомной эры» в конце 1940-х годов. Одним из методов защиты от ядерных ударов было создание наземных генераторов радиолокационных помех, чье излучение могло «обмануть» радиолокационный высотометр ядерной бомбы и привести к несвоевременному или некорректному срабатыванию механизма инициации[92]. Весьма вероятно, что эта борьба радиоэлектронного «меча» и «щита» продолжается.

Полноценная автономность является прорывной технологией и для боевых действий в океанских глубинах. Например, океанская многоцелевая система может быть использована как средство доставки ядерных боезарядов, по информации некоторых источников, сверхкрупного, мегатонного класса, что вместе с тем создает угрозу катастрофических последствий выхода из-под контроля подобной системы в связи с враждебным кибервоздействием[93]. Другой угрозой (причем, как под водой, так и в иных средах), является непреднамеренное столкновение нескольких автономных систем различных вероятных противников. Как поведут себя «ядерные роботы» в такой ситуации предсказать сложно, однако в случае агрессивного взаимодействия, вероятно, могут осуществляться попытки атаки с использованием ИКТ. Таким образом, как продвинутой СПРН, использующей автоматический анализ информации из различных источников, так и интеллектуальной системе поддержки управленческих решений в области материально-технического обеспечения можно навязать наборы заведомо искаженных данных («атака пятого типа»). Такое действие может привести в первом случае к неверной оценке обстановки и, как следствие, неверному реагированию. Во втором случае результатом такой атаки может стать выход из строя вооружений и военной техники и соответствующее разрушение ядерного потенциала. Полностью автоматизированный процесс нанесения ответного ядерного удара технологически осуществим, и в случае стремительной деградации стратегической стабильности решение о предварительном делегировании полномочий автономным подсистемам вполне

[91] Влияние искусственного интеллекта на стратегическую стабильность и ядерные риски / Под ред. В. Буланина. – СИПРИ, 2019. С. 94-95.
[92] Кини Л. 15 минут: Генерал Кертис ЛеМэй и обратный отсчет до ядерной аннигиляции. – Нью-Йорк, 2011. С. 46.
[93] Подводный аппарат «Посейдон» сможет нести боеголовку мощностью до двух мегатонн // ТАСС. 2018. 17 мая. URL: https://tass.ru/armiya-i-opk/5208267.

может быть принято – но в такой ситуации весь спектр ИКТ-угроз представляет собой совершенно апокалиптические риски.

Вместе с тем ключевой угрозой как для автоматизированного возмездия, так и для отдельных автономных носителей ЯО представляется ввод в системы обработки данных заведомо ложной информации («атака пятого типа»), ведущей к некорректному функционированию соответствующих аналитических подсистем.

4.3. Проблема атрибуции компьютерных атак в процессе обеспечения стратегической стабильности

В условиях глобальной цифровизации число киберинцидентов и кибератак увеличивается[94], часть из них имеют серьезный общественный резонанс, поскольку наносят реальный экономический, технологический, военный или политическим ущерб. Ряд отдельных киберинцидентов в ракетно-ядерной и космической сферах уже инициировал дебаты по стратегической стабильности в мире[95]. Вспомним, что в преддверии XXI века кибератаки и кибероперации характеризовались относительно неявным политическим и экономическим ущербом, но в 2010 году ситуация принципиально изменилась в связи с идентификацией и последующим анализом кибероперации «Олимпийские игры» (*Stuxnet*), в результате которой, как утверждалось, была приостановлена ядерная госпрограмма Ирана. Это резко повысило актуальность ряда вопросов международной информационной безопасности (МИБ).

Как государству реагировать на компьютерные атаки, приводящие к существенному ущербу?

Какие допускаются ассиметричные меры предупреждения и сдерживания?

Что делать, чтобы избежать эскалации конфликта?

Возможно ли регулирование международной информационной безопасности?[96]

К сожалению, применение традиционных международных мер правового и технического регулирования в области международной безопасности и стратегической стабильности к ИКТ-пространству затруднено по причине феноменальных особенностей виртуального киберпространства и присущей интернету технической организации доступа к его ресурсам. Так, киберпространство не имеет четких физических границ, что затрудняет, например, демаркацию и делимитацию. Технические правила интернета поддерживают различные варианты анонимизации, что усложняет контроль деятельности субъектов международного права. Программные приложения характеризуются чрезвычайно высоким уровнем структурной сложности, что не дает возможности применять точные методы анализа и обусловливает рост информационных рисков, уязвимостей и пр. Все это определяет высокий уровень неопределённости при решении комплекса задач международной безопасности, и главным образом, при идентификации и аутентификации источников (субъектов) атак в киберпространстве. Названная проблема в области международного сотрудничества получила название атрибуции кибератак (*cyber-attack attribution, cyber attribution*).

---

[94] Андрей Крутских рассказал о количестве кибератак на объекты критической инфраструктуры России // Международная жизнь/ 2020. 28 июня. URL: https://interaffairs.ru/news/show/26787.

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

[96] Axelrod R., Iliev R. Timing of cyber conflict // PNAS. – Vol. 111 (2014). – No 4. – P. 1298–303; Fitton O. Cyber Operations and Gray Zones: Challenges for NATO // Connections QJ. – Vol. 15 (2016). – No. 2. – P. 109-119. DOI: 10.11610/Connections.15.2.08.

4.3.1. Понятийный аппарат

Происхождение термина ***атрибуция*** берет начало с латинского *attributio* – приписывание (констатация, установление), термин давно устоялся в сферах авторского права (предписание авторской принадлежности), журналистики (выявление источника информации), искусствоведении и филологии (установление подлинности и авторства) и др. Что касается ***атрибуции кибератак***, то дефиниция в настоящее время находится на этапе становления, ее еще нет в терминологических глоссариях технических подкомитетов, сообществ и служб по защите информации, таких как IEC, ISO, NIST, ГОСТ, ISACA, FOIS/BSI. В литературе атрибуцию кибератак в целом трактуют как комплекс процедур по выявлению источника атаки с целью возложения ответственности. Приведем определения академических аналитиков и технических экспертов. Так, стэндфордская группа ученых[97] считает, что атрибуция – это процесс, с помощью которого доказательства происхождения киберинцидента собираются, оцениваются и приписываются ответственному субъекту или физическому лицу. Международная компания «Лаборатория Касперского» под атрибуцией понимает комплекс технических методов и организационных мер по выявлению лиц, совершивших кибератаку или вредоносную кампанию, но при этом указывается, что атрибуция, как правило, предполагает проведение экспертизы следов киберпреступлений, а также следственные действия на основе выводов аналитиков[98].

Указанный терминологический подход отражает и технологические, и международно-правовые моменты. Исходя из этого, условно атрибуцию кибератак можно разделить на: техническую (криминалистическую), выполняющую функцию определения; политическую (правовую, дипломатическую), выполняющую предписывающую функцию.

4.3.2. Сложности атрибуции кибератак

Отметим барьеры, которые обусловили сложность разрешения проблемы атрибуции кибератак, а именно: политический, правовой, организационно-технический и технический уровни.

На политическом уровне атрибуция кибератак представляет собой пока скорее инструмент информационного противоборства, а не идиллии международного сотрудничества. Здесь можно наблюдать недоказуемые обвинения и тривиальное отрицание причастности, а также разного рода взбросы и фейки.

Правовой уровень международных отношений, по оценкам ряда ученых[99], представляет собой также пока «серую зону» античного международного права, сформированного изначально в конкретном физическом мире. Например, в киберпространстве нет общей трактовки военного агрессора (например, по Клаузевицу – применяющего физическое насилие к людям). Отсюда нет четкого понимания, какие допустимы контрмеры защитного, сдерживающего или наступательного характера. Как уже упоминалось, неясно как провести делимитацию и демаркацию в виртуальном пространстве.

Организационно-технические барьеры состоят в том, что в настоящее время нет никаких международных организационных стандартов по взаимному мониторингу и контролю действий и деанонимизации в Интернете. В то же время, в ряде стран (например, в Китае) имеется опыт по правовому и техническому регулированию действий в киберпространстве сегмента страны.

---

[97] Attribution.news. URL: https://attribution.news/about/.
[98] Cyber Attribution. URL: https://encyclopedia.kaspersky.com/glossary/cyber-attribution/.
[99] Fitton O. Указ. соч.

Технические проблемы изначально присущи Интернету, организация которого не ориентирована на запрет анонимности в каком бы то ни было виде. К основным недостаткам метасети относят следующие: в принципе децентрализованная сегментируемая архитектура, ограничения адресации IPv4, разного рода средства и сервисы анонимизации. Более того, структурная сложность программных средств является объективной причиной для уязвимости сетевых подсистем, что может привести к подмене идентификационно-адресной информации или обходу подсистем аутентификации и регистрации.

Можно добавить еще ряд негативных причин, тормозящих разрешение проблемы атрибуции, например, коммерческие причины скрытия инцидента и банальный непрофессионализм.

4.3.3. Современная исследовательская база

Исследовательская база этой проблемы представлена наиболее активными в рассматриваемой области компаниями и организациями, которые публично представили обзоры по атрибуции (таблица 4.2). В связи с тем, что сотня стран имеет подразделения по кибербезопасности, а 99% кибероперациий приходится на 10 стран, можно предположить, что ряд стран скрывают свои исследования. Это значит, что большинство представленной аналитики может иметь односторонний политический подтекст.

Таблица 4.2. Источники отчетов по атрибуции

Организация	Страна	Тип организации	Пример интернет-источника
Cisco (Talos)	США	Публичная компания	https://blog.talosintelligence.com/2018/02/group-123-goes-wild.html
CrowdStrike Holdings	США	Публичная компания	www.crowdstrike.com/blog/meet-the-adversaries/
FireEye (Mandiant)	США	Публичная компания	www.fireeye.com/current-threats/apt-groups.html
MITRE	США	Некоммерческая организация	
NSA	США	Федеральная служба	www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/
Secureworks (Dell)	США	Публичная компания	www.secureworks.com/research/threat-profiles
Лаборатория Касперского	Россия	Акционерное общество	www.securelist.com/all/?category=908

Источник: таблица построена автором.

4.3.4. Основы технической атрибуции

Само название «атрибуция» подразумевает сбор и оценку значимости собственно атрибутов (признаков, факторов) кибератак, на основании чего делается вывод об ответственности (с некоторой степенью уверенности). Так как нет правовых соглашений в области международной атрибуции кибератак (кроме этических деклараций), то фактически нет ограничений по сбору атрибутивных данных. В реальности они могут быть получены легитимным и нелегитимным путем

(например, из darknet), прямо или косвенно, с применением технических и нетехнических средств. Типовыми процедурами сбора атрибутов могут быть анализ программного кода, изучение системных журналов и мониторинг трафика, анализ доступных в интернете данных (OSINT), слежка и перехват информации техническим и оперативным путем, а также использование ловушек (honeypot, «серых сетей» и т.д.) и иных форм провокаций и пр. Это означает, что полученная информация из различных источников обладает различным уровнем достоверности и публичности.

4.3.5. Классификация технической атрибуции

В киберсреде предлагается следующая классификация атрибутов: особенности программных ресурсов; особенности сетевой активности; методические особенности атаки; данные о субъектах атаки; иная информация, полученная без использования собственно компьютерных сетей, например, техническая и агентурная разведка, аналитика по косвенным причинам, разного рода провокации и т.д.

К атрибутам программных ресурсов можно отнести: наборы уязвимостей, повторно используемых злоумышленниками; наличие уязвимостей нулевого дня; наследование вредоносного кода; артефакты в программном коде; особенности приемов и стиля программирования; стилистика комментариев.

К атрибутам сетевой активности можно отнести: место регистрации сетевых адресов и доменов, участвующих в кибератаке; особенности ИТ-инфраструктуры управления вредоносным ПО; использование бот-сети; результаты обратной трассировки.

К атрибутам методики кибератаки можно отнести: дополнительные тактические (и этические) приемы хакерских группировок; целевые объекты атак (страны/территории, отраслевая направленность мотивации, серии платформ и физическая адресация, неприкасаемые объекты); временные последовательности.

К атрибутам субъектов атаки, в первую очередь, следует отнести вычисление специалистов, задействованных в кибероперации.

Пример атрибуции кибератак с использованием предложенной классификации, которая демонстрирует наиболее значимые факторы атак, представлена в таблице 4.3.

4.3.6. Пример атрибуции по наследованию программного кода

Ярким примером идентификации факта наследования вредоносного кода (АЗ) стали результаты анализа целенаправленных вредоносных программ – кибероружия *Stuxnet* (2009 год) и *Flame* (2010 год), задействованных в известных кибероперациях, когда в их коде был найден модуль эксплойта червя *Fanny* (2008 год), исходный текст которого был случайно обнаружен на ресурсах Агентства национальной безопасности (АНБ) США, что стало значимой уликой в обвинениях в адрес США[100]. О связи *Stuxnet* с АНБ и ЦРУ было достаточно признаний бывших сотрудников спецслужб США[101].

[100] Мощнее Stuxnet и Flame: «Лаборатория Касперского» обнаружила самого сильного на данный момент игрока в мире кибершпионажа // Kaspersky. 2015. 17 февраля. URL: https://www.kaspersky.ru/about/press-releases/2015_moshhnee-stuxnet-i-flame.

[101] Nakashima E., Warrick J. Stuxnet was work of U.S. and Israeli experts, officials say // The Washington Post. 2012. 2 июня. URL: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Таблица 4.3. Пример классификации и атрибуции кибератак

Название	Уязвимость (A1)	Программы (A3)	Цели (C3)	Источник (B1)	Тактические приемы (C1)	Группа
Атака на посетителей форумов, посвященных исламскому джихаду	Уязвимость в Firefox 17 (TOR Browser)	Неизвестный эксплойтйф	В список целей не включены IP-адреса Иордании, Турции и Египта, но включены пользователи конкретного провайдера спутникового интернета в Афганистане	Серверы Equation Group	Атаке подвергались только авторизованные пользователи, которые зашли с определенных IP-адресов	Equation Group (США)
Атака на правитель-ственные организации с использова-нием уязвимости CVE-2017-11882	Уязвимость в Microsoft Office CVE-2017-11882	Backdoor, написанный на PowerShell-POWRUNER	ЦЙ2ФФФФФ	н/д	Массовые рассылки сообщений с использованием скомпрометиро-ванных учетных записей. Социальная инженерия.	APT 34 (Иран)

Источник: таблица построена автором.

4.3.7. Пример атрибуции по вычислению специалистов

Зачастую тщеславие, ошибки и оплошности человека могут служить причиной его личной идентификации с последующими выводами. Примером вычисления специалиста (атрибут D1), задействованного в кибероперации, является атрибуция, выполненная организацией FireEye[102]. Псевдоним пользователя *UglyGorilla*, под которым он участвовал в полемике о кибервойсках в Китае, в рамках атрибуции был обнаружен во вредоносном программном обеспечении: «v1.0 No Doubt to Hack You, Writed by UglyGorilla, 06/29/2007», а для организации управления кибероружием использовались доменные имена, содержащие UG: ug-opm.hugesoft.org, ug-rj.arrowservice.net, ug-hst.msnhome.org.

Исследование показало, что этот же пользователь зарегистрирован на форуме военнослужащих chinamil.com.cn (под ником *UglyGorilla* с указанием реального отчества Wang, что, якобы, принято в Китае). Позже человек с таким же псевдонимом *UglyGorilla* и отчеством Wang загрузил на сайт, посвященный разработке программ, свой вредоносный код (*mailbomb*). Указанное (по совокупности с другими атрибутами) позволило легко возложить ответственность за серию APT-атак на Китай, точнее, на воинскую часть 61398 (ныне классифицируется как хакерская группа APT1).

Как это принято в обычных расследованиях, компьютерные детективные процедуры зачастую позволяют сузить круг подозреваемых, которые затем могут быть проверены, например, оперативным путем. При этом существует озабоченность по поводу влияния компьютерной разведки на международную безопасность и стабильность. Опуская полемику об интернет-протоколах, системные

[102] Exposing One of China's Cyber Espionage Units // Mandiant, 2010. URL: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

среды и электронику, отметим, что зачастую облачные технологии, широко задействованные в киберфизических системах и персональных гаджетах, принадлежат узкому кругу ряда супердержав. Слияние (в перспективе технологическая сингулярность) указанных технологий с достижениями в области супервычислений и когнитивных вычислений могут обусловить глобальное преимущество в киберпространстве в целом и в решении задачи атрибуции, в частности. Что касается политических деклараций, то министр обороны США и ряд его коллег часто заявляют на политической арене, что спецслужбы США располагают технической возможностью решения проблемы атрибуции.

4.3.8. Таксономия MITRE

В настоящее время в области технической атрибуции стала популярна база тактик и техник хакерских групп (ATT&CK – Adversarial Tactics, Techniques & Common Knowledge), которая поддерживается международной некоммерческой организацией MITRE. Типы таксонов представлены в таблице 4.4, основная идея таксономии – на рисунке 4.6. Несмотря на статус международной, надо понимать, что MITRE является проектом США, то есть не содержит данных, связанных с кибероперациями США, их союзников и партнеров.

4.3.9. Проблемы политической атрибуции

Техническая атрибуция носит в целом объективный характер, так как основывается на конкретных технических данных, однако использование количественных критериев и показателей в любом случае затруднено по названным ранее причинам. Уровень неопределенности существенно повышает действия по скрытию и маскировке, особенно маскировке под третьих лиц («под чужим флагом»).

Что касается геополитической области, в условиях отсутствия соответствующей нормативно-правовой договоренности атрибуция носит выраженный субъективный характер, основанный на экспертном анализе информации в контексте политических задач. Фактически, политическая атрибуция выражает поставленные государственные задачи, касающиеся, например, нанесенного политического и экономического ущерба. Ряд известных ученых философски считают, что атрибуция – это «то, что государства делают из этого» и это «функция того, что поставлено на карту с политической точки зрения»[103]. По оценкам некоторых ученых политическая атрибуция в настоящее время невозможна, но из этого не следует, что надо избегать создания системы нормативно-правового регулирования[104].

Можно назвать типовые проблемные вопросы политической атрибуции: обвиняемое государство отрицает причастность к компьютерной атаке; обвиняемое государство отрицает связь с идентифицированными субъектами атаки, действующими с его территории; обвиняющее государство затрудняется обосновать уровень ответных действий (защита, сдерживание, наступательные действия) в киберпространстве; обвиняющее государство затрудняется обосновать возможность применения кинетического оружия в ответ на недружелюбные действия в

[103] Rid T., Buchanan B. Attributing Cyber Attacks // The Journal of Strategic Studies. – 2015. – Vol. 38 (2015). – No. 1–2, 4–37. DOI: 10.1080/01402390.2014.977382.

[104] Стрельцов А.А. Суверенитет и юрисдикция в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. 2017. № 2. С. 87-106. Шерстюк В.П., Крутских А.В., Плохой О.А. и др. Сборник докладов участников Тринадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (22–25 апреля 2019, Гармиш-Партенкирхен, Германия). – НАМИБ, 2020.

виртуальном пространстве. В таблице 4.5 приведено сравнение технической и дипломатической атрибуции.

Таблица 4.4. Набор методических приемов хакерских групп, систематизированных MITRE (8.07.2020)

Способы, методические приемы атаки	Число способов
Начальный доступ	9
Выполнение кода	10
Обеспечение присутствия	18
Повышение привилегий	12
Обход механизмов безопасности	34
Получение удостоверяющих данных	14
Разведка ресурсов	24
Горизонтальные действия	9
Сбор данных	16
Управление	16
Вывод данных (эксфильтрация)	9
Воздействие	13

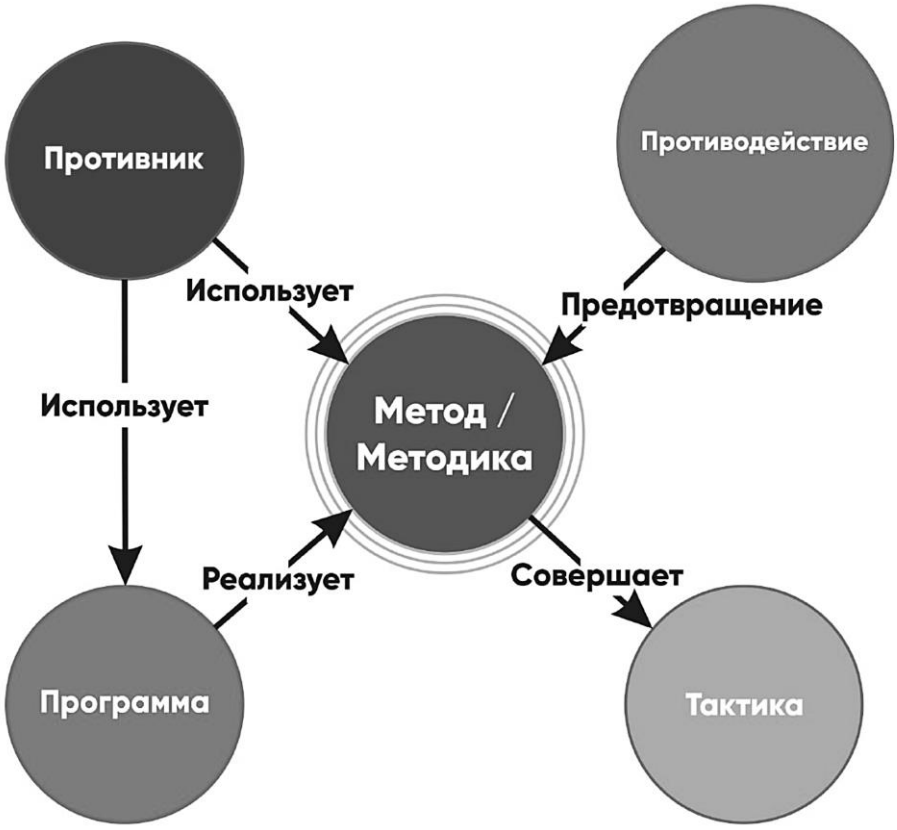
Источник: mitre.org.

Таблица 4.5. Сравнение характеристик технической и политической атрибуций

Тип	Функция	Достоверность	Базовые методы	Показатели, критерии
Техническая (криминалисти-ческая)	Определения (детективная)	Высокая	Мониторинг, контроль ресурсов и процессов	Количественные качественные
Политическая (нормативная, дипломатическая)	Предписывающая	Низкая	Соблюдение норм, анализ мотивации	Качественные (highly likely)

Источник: таблица построена автором.

Рисунок 4.7. Онтология ATT&CK



Источник: mitre.org.

4.3.10. Модели атрибуции

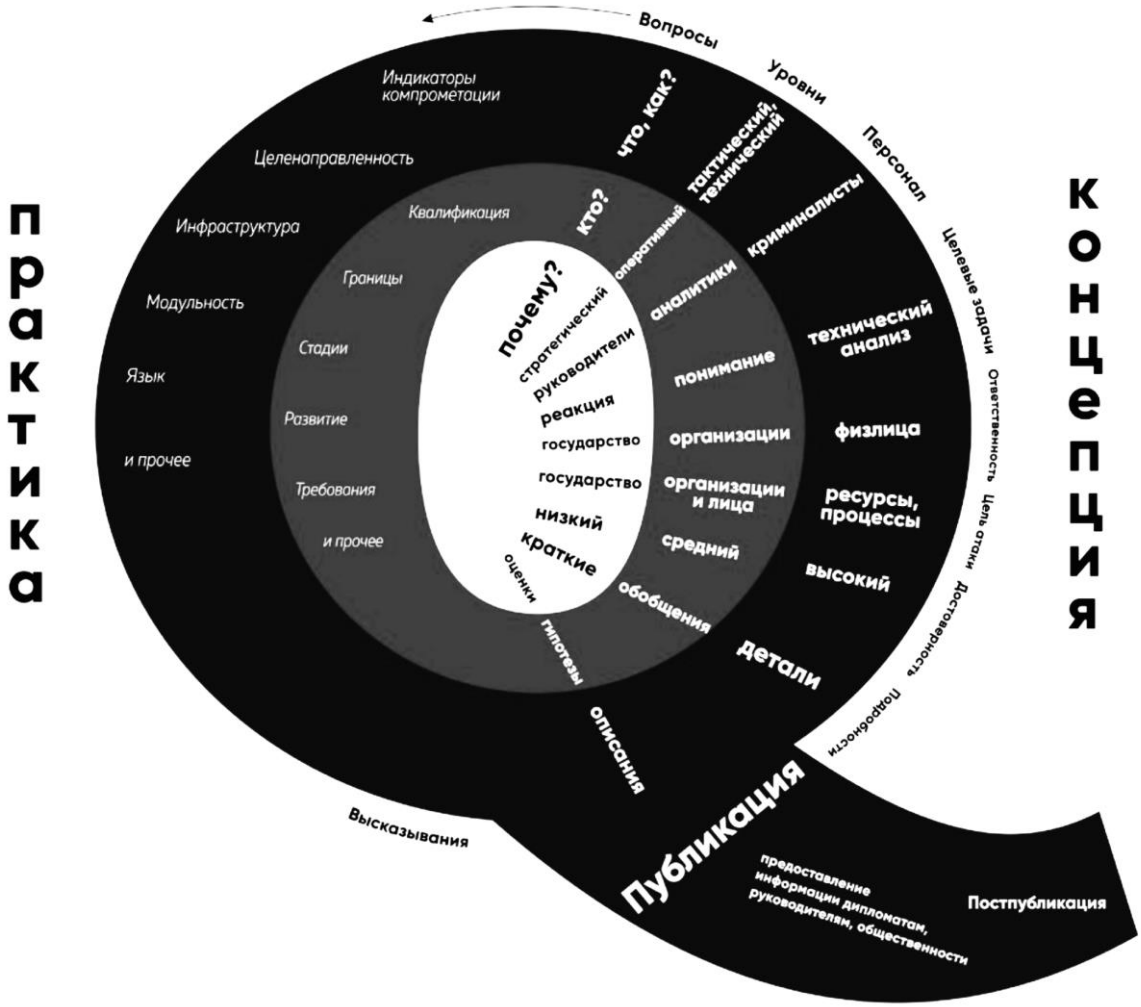
В литературе можно встретить ряд концептуальных моделей атрибуции, позволяющих получить отдельные оценки показателей качества процесса атрибуции и доверия к решению по возложению ответственности. Наиболее дискутируемой является так называемая Q-модель, предложенная в работе Attributing Cyber Attacks. Модель носит описательный концептуальный характер аналитического «мозгового» цикла (гипотеза-обсуждение-действие).

Она основана на следующих допущениях и положениях:

- процесс атрибуции носит сложный (нелинейный) и частично итерационный характер;
- процесс атрибуции проходит на трех взаимосвязанных уровнях: тактическом (как технически происходила атака), оперативном (как организационно происходила атака) и стратегическим (какие могут быть мотивы и т.п.);
- процесс атрибуции завершается процессом коммуникации: принятием решения о публичности;
- результативность атрибуции ограничена ресурсами (технологическими, экономическими, временными, квалификационными), которые в том числе релевантными ущербу;
- аналитический разбор подзадач атрибуции состоит в помощи ответственным лицам принимать взвешенные решения, при этом заключения характеризуются неким уровнем неопределенности.

Визуально сложный процесс сбора и анализа данных представляется тремя кольцами, а вывод (в виде решения на опубликование вердикта) креативно иллюстрирует хвостом буквы Q (рисунок 4.8).

Рисунок 4.8. Q-модель атрибуции кибератак



Источник: Rid T., Buchanan B. Attributing Cyber Attacks // The Journal of Strategic Studies. – 2015. – Vol. 38 (2015). – No. 1–2, 4–37. DOI: 10.1080/01402390.2014.977382.

4.3.11. Нормативное и техническое регулирование

Несмотря на сложность атрибуции и присущие этому процессу барьеры, очевидно, что в условиях международного сотрудничества следует стремиться к договоренностям, а в итоге – к регулированию процесса международной безопасности и стабильности в киберпространстве. Можно предложить, например, ряд решений в данной области.

Дипломатические направления по повышению эффективности атрибуции:

1) выполнение соглашений группы правительственных экспертов ООН;
2) осуществление взаимодействия между группами CERT различных стран;
3) организация экспертного сообщества исследователей для совместной выработки решений на основе различных интересов и подходов;

4) осуществление взаимодействия на политическом и техническом уровнях для расследования инцидентов;
5) создание консультационных механизмов для повышения доверия;
6) усиление защиты критически важной инфраструктуры;
7) международное взаимодействие по обмену информацией об инцидентах, их характерных признаках и степени их угроз;
8) соглашение о запрете кибератак на элементы информационной инфраструктуры.

Организационно-технические направления по повышению эффективности атрибуции:

1) использование на узлах информационной инфраструктуры стран модулей, обеспечивающих механизмы подписи данных;
2) подпись и децентрализованное хранение журналов;
3) дополнение трафика специальной информацией, содержащей подпись наблюдателя;
4) передача дополнительных подписанных сообщений о трафике;
5) внесение неопределенности для злоумышленника (изменение конфигурации, использование сетевых ловушек, использование водяных знаков, раскрывающих злоумышленника);
6) применение общей распространенной структуры систем обнаружения вторжений с общими актуальными международными базами правил;
7) ведение реестра злоумышленников.

ЗАКЛЮЧЕНИЕ

Стремительное развитие ИКТ идет много лет, продолжается их внедрение во все виды и рода вооруженных сил. Это здоровый и в целом позитивный процесс. Однако изучение угроз в этой области и своевременное реагирование на выявленные проблемы, допустимая транспарентность в области конкретных решений и демонстрации успехов должны сопровождать научно-технический прогресс в военной области.

Самые опасные информационные угрозы международной безопасности и стабильности: применение ИКТ-оружия в военно-политических целях для осуществления враждебных действий и актов агрессии; деструктивное ИКТ-воздействие на элементы критически важных объектов государственной инфраструктуры; вмешательство во внутренние дела суверенного государства, снижение общественной стабильности, разжигание межэтнической и межнациональной розни посредством ИКТ. Наличие этих опасностей требует поиска дополнительных механизмов международного управления.

В контексте обеспечения стратегической стабильности особого внимания требует безопасность ракетно-ядерных вооружений. Все ядерные державы модернизируют их, стремясь внедрять новые компьютерные технологии. Все больше компонентов военной ядерной инфраструктуры – от боеголовок и средств их доставки до систем управления и наведения, систем связи, командования и контроля над ядерными силами – зависят от сложного программного обеспечения, что делает их потенциальными мишенями для ИКТ-атак.

Это порождает потенциальные риски, связанные, в частности, с ростом вероятности:

- ошибочного санкционированного пуска баллистических ракет или предотвращения (блокирования) пуска;
- получения ложной информации от СПРН о запуске баллистических ракет со стороны противника из-за растущей изощренности ИКТ-атак;
- повреждения или разрушения каналов коммуникаций, создания помех в системе управления, командования и контроля ВС;
- снижения уверенности военных, принимающих решения, в работоспособности систем и восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения.

Нельзя однозначно определить какие-то отдельные элементы ядерных сил, в наибольшей степени подверженные ИКТ-угрозам. Однако можно определить факторы, оказывающие наибольшее влияние на уязвимость. К таковым следует отнести: взаимодействие с «сетями общего пользования»; географию боевого дежурства; элементную базу; наличие «искусственного интеллекта»; квалификацию операторов; «человеческий фактор». В любом случае защита стратегических вооружений, систем СПРН, ПВО и ПРО, связи, командования и контроля над ядерным оружием от ИКТ является актуальной глобальной проблемой современности.

В связи с этим целесообразно проводить регулярную экспертную оценку и переоценку уровня ИКТ-угроз в отношении различных систем и подсистем управления и боевого применения ядерного оружия.

В связи с масштабом угроз и катастрофическими последствиями реализации ИКТ-угроз для ядерного оружия необходима активная работа внешнеполитических ведомств по согласованию на международном уровне перечней критической инфраструктуры ядерных сил, попытка воздействия на которую с применением ИКТ

будет расцениваться как попытка обезоруживающего удара с соответствующими последствиями для атаковавшей стороны.

Важным шагом к включению темы угроз в сфере ИКТ в диалог по стратегической стабильности может стать подготовка соответствующего раздела в «Глоссарий ключевых ядерных терминов», о доработке которого «ядерная пятерка» договорилась в ходе конференции в Вашингтоне в сентябре 2016 года[105].

Параллельно с этим необходимо продолжить в ООН работу по формированию режима контроля над ИКТ-вооружениями, который мог бы включать:

- конкретные меры укрепления доверия и безопасности в ИКТ-сфере;
- запрет ИКТ-атак на конкретные объекты, в том числе в военной сфере ив особенности – ядерные;
- ограничение и (или) отказ от наступательных ИКТ-возможностей;
- меры контроля за распространением ИКТ-вооружений;
- международные нормы в отношении средств и методов предотвращения и устранения киберконфликтов;
- разработку конвенции о запрещении вредоносного использования ИКТ в сфере ЯО.

[105] Joint Statement from the Nuclear-Weapons States at the 2016 Washington. DC P5 Conference, Washington, DC, September 15, 2016 // The Ministry of Foreign Affairs of the Russian Federation URL: https://www.mid.ru/web/guest/adernoe-nerasprostranenie/-/asset_publisher/JrcRGi5UdnBO/content/id/2451010.

БИБЛИОГРАФИЯ

Монографии

1. Барсенков А.С., Веселов В.А., Есин В.И., Шеремет И.А. Вопросы обеспечения стратегической стабильности в советско-американских и российско-американских отношениях: теоретические и прикладные аспекты. – М.: МГУ, 2019. – 144 с.
2. Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева, И.В. Авчаров, А.В. Бедрицкий и др.; под ред. А.В. Фёдорова, В.Н. Цыгичко. – М.: ПИР-Центр, 2001. – 328 с.
3. Лысенко Н. Наведение баллистических ракет. – М.: МГТУ им. Н.Э. Баумана, 2016. – 448 с.
4. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении / Под общей ред. С.Ф. Боева; вводные слова А.И. Смирнова и А.Г. Тормасова; вводная статья И.А. Каляева. - Иннополис: Издательский Дом «Афина», 2017. – 440 с.
5. Проблемы информационной безопасности в международных военно-политических отношениях / Под ред. А.В. Загорского, Н.П. Ромашкиной. – М.: ИМЭМО РАН, 2016. – 183 с. DOI: 10.20542/978-5-9535-0477-5.
6. Ромашкина Н.П. Стратегическая стабильность в современной системе международных отношений. М.: Научная книга, 2008 – 288 с.
7. Россия и дилеммы ядерного разоружения / Под ред. А.Г. Арбатова, В.З. Дворкина, С.К. Ознобищева. – М.: ИМЭМО РАН, 2011. – 237 с.
8. Суперкомпьютерные технологии в науке, образовании и промышленности / Под ред. В.А. Садовничего, Г.И. Савина, Вл.В. Воеводина. – М.: Издательство Московского университета, 2009. – 232 с.
9. Угрозы информационной безопасности в кризисах и конфликтах XXI века / Под ред. А.В. Загорского, Н.П. Ромашкиной. – М.: ИМЭМО РАН, 2015 – 151 с.
10. Ядерное распространение: новые технологии, вооружения и договоры / под ред. А. Арбатова, В. Дворкина; Моск. Центр Карнеги. – М.: Российская политическая энциклопедия (РОССПЭН), 2009. — 272 с.
11. Clarke R.A., Knake R. Cyber War: The Next Threat to National Security and What to Do about It. – New York: HarperCollins, 2010. – 320 p.
12. Futter A. Hacking the Bomb: Cyber Threats and Nuclear Weapons. – Georgetown: Georgetown University Press, 2018. – 208 p.
13. Harris S. @War: The Rise of the Military-Internet Complex. – Boston: Houghton Mifflin Harcourt, 2014. – 263 p.
14. Keeney L. D. 15 Minutes: General Curtis LeMay and the Countdown to Nuclear Annihilation. – New York: St. Martin's Press, 2011. – 400 p.
15. Petrenko S. Cyber Security Innovation for the Digital Economy a Case Study of the Russian Federation. - River Publishers, 2018. – 492 p.
16. Probabilistic Modeling in System Engineering / A. Kostogryzov (ed.). – London: IntechOpen, 2018 – 290 p. DOI: 10.5772/intechopen.71396.
17. Wheeler D. A., Larsen G. N. Techniques for Cyber Attack Attribution. – Alexandria, VA: Institute For Defense Analyses Alexandria, 2003. 84 p.

Статьи

1. Арбатов А. Г. Угрозы стратегической стабильности – мнимые и реальные // Полис. Политические исследования. – 2018. – № 3. – С. 7-29. DOI:10.17976/jpps/2018.03.02.
2. Арбатов А.Г. Роль ядерного сдерживания в стратегической стабильности. Гарантия или угроза / Московский Центр Карнеги. 2019. 28 января. URL: https://carnegie.ru/2019/01/28/ru-pub-78209.
3. Арбатов А.Г. Разоружение – утопия или императив поствильсоновской эпохи? // 14 пунктов» Вильсона сто лет спустя: как переизобрести мировой порядок. – М.: ЦСП, 2018. С. 50-58. URL: https://www.csr.ru/upload/iblock/911/9111f855a2ef1624332e9c87c6f50f2d.pdf.
4. Арбатов А.Г. Ядерный потолок // Военно-промышленный курьер ВПК. – 2014. – № 26 (544). 23 июля. С.4-5. URL: https://www.vpk-news.ru/articles/21133.
5. Барабанов А. В., Марков А. С., Цирлов В. Л. Актуальные вопросы выявления уязвимостей и недекларированных возможностей в программном обеспечении // Системы высокой доступности. – 2018. – Т. 14. – №. 3. – С. 12-17. DOI: 10.18127/j20729472-201803-03.
6. Барабанов А.В., Марков А.С., Цирлов В.Л. О систематике информационной безопасности цепей поставки программного обеспечения // Безопасность информационных технологий. – 2019. – Т. 26. – № 3. DOI: 10.26583/bit.2019.3.06.
7. Бендерский Л. А., Любимов Д. А., Рыбаков А. А. Анализ эффективности масштабирования при расчетах высокоскоростных турбулентных течений на суперкомпьютере RANS/ILES методом высокого разрешения // Труды научно-исследовательского института системных исследований Российской академии наук. – 2017. – Т. 7. – №. 4. – С. 32-40.
8. Бойко С.М. Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Международная жизнь. – 2018. – № 11. – С.23-35.
9. Гареев М. А., Турко Н. И. Война: современное толкование теории и реалии практики // Вестник Академии военных наук. – 2017. – №. 1. – С. 4-10.
10. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. – 2019. – № 3 (31). – 18-23. // DOI: 10.21681/2311-3456-2019-3-18-23.
11. Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. – 2007. – Т. 5. – №. 13. – С. 28-37.
12. Крутских А. В., Стрельцов А. А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. – 2014. – №. 11. – С. 20-34.
13. Лукацкий А. В. Определение источника кибератак // Индекс безопасности. – 2015. – Т. 21. – №. 2. – С. 73-86.
14. Марков А. С., Шеремет И. А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник академии военных наук. – 2019. – №. 2. – С. 82-90.
15. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. – 2013. – № 1. – С. 28-36.
16. Петренко А.А., Петренко С.А. НИОКР агентства DARPA в области кибербезопасности // Вопросы кибербезопасности. – 2015. – № 4 (12). – С. 2-22.

17. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. – 2019. – №. 1 (29). – С. 2-9. DOI: 10.21681/2311-3456-2019-1-2-9.
18. Ромашкина Н.П. Новые технологии: вызовы международной безопасности и стабильности // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2019. – С. 329 – 334.
19. Ромашкина Н.П. Стратегическая стабильность: новые вызовы инфосферы // Российский совет по международным делам. 2017. 23 ноября. URL: https://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-stabilnost-novye-vyzovy-infosfery/.
20. Россия и глобальные вызовы в области информационной безопасности. XII Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» Гармиш-Партенкирхен, Германия 16–19 апреля 2018 года // Международная жизнь, 2018. Спецвыпуск. – 180 с. URL: https://interaffairs.ru/virtualread/garmish2018/publication.pdf.
21. Сангалов В. А. Угрозы национальной безопасности России в информационной сфере // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2015. – №. 8-3. – С. 161-167.
22. Стефанович Д. В. Космос как предчувствие //Россия в глобальной политике. – 2020. – Т. 18. – №. 5. – С. 187-196.
23. Стефанович Д.В. Ядерно-кибернетические комплексы // Российский совет по международным делам. – 2017. 06 июля. .07.2017. URL: https://russiancouncil.ru/analytics-and-comments/analytics/yaderno-kiberneticheskie-kompleksy/.
24. Стефанович Д.В. Ядерное измерение киберугроз // Российский совет по международным делам. 2019. – 5 августа. URL: https://russiancouncil.ru/analytics-and-comments/analytics/yadernoe-izmerenie-kiberugroz/.
25. Стрельцов А. А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. – 2017. – №. 2. – С. 87-106.
26. Стрельцов А. А., Смирнов А. И. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям //Международная жизнь. – 2017. – №. 11. – С. 71-81.
27. Шерстюк В. П. XIV Научная конференция Международного исследовательского консорциума информационной безопасности // Международная жизнь. – 2017. – №. 14. – С. 42-180.
28. Axelrod R., Iliev R. Timing of cyber conflict // Proceedings of the National Academy of Sciences. – 2014. – Vol. 111. – №. 4. – P. 1298-1303.
29. Barabanov A. V., Markov A. S., Tsirlov V. L. Statistics of software vulnerability detection in certification testing // Journal of Physics: Conference Series. – 2018. – Vol. 1015. – №. 4. DOI: 10.1088/1742-6596/1015/4/042033.
30. Dacier M., Pham V. H., Thonnard O. The WOMBAT Attack Attribution method: some results // International Conference on Information Systems Security. –Berlin, Heidelberg: Springer, 2009. – P. 19-37.
31. Fitton O. Cyber operations and gray zones: Challenges for NATO // Connections. – 2016. – Т. 15. – №. 2. – P. 109-119. DOI: 10.11610/Connections.15.2.08.

32. Grotto A. Deconstructing Cyber Attribution: A Proposed Framework and Lexicon // IEEE Security & Privacy. – 2019. – Т. 18. – №. 1. – P. 12-20. DOI:10.1109/MSEC.2019.2938134.
33. Howard M., Lipner S. The Security Development Lifecycle: A Process for Developing Demonstrably More Secure Software. – Microsoft Press, 2006. – 25 p.
34. Lin H. Attribution of malicious cyber incidents: From soup to nuts. Hoover Working Group on National Security, Technology, and Law. Aegis Series Paper No 1607. 2016. 26 September. – 56 p. URL: https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.
35. Markov A.S., Sheremet I.A. Enhancement of Confidence in Software in the Context of International Security // CEUR Workshop Proceedings. – 2019. – Vol. 2603. – P.88-92.
36. Mulvenon J. Toward a cyberconflict studies research agenda // IEEE Security & Privacy. – 2005. – Vol. 3. – №. 4. – P. 52-55.
37. Nunes E. et al. Argumentation models for cyber attribution // 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). – IEEE, 2016. – P. 837-844.
38. Reed M., Miller J. F., Popick P. Supply chain attack patterns: Framework and Catalog // Office of the Deputy Assistant Secretary of Defense for Systems Engineering. – 2014. – 88 p. URL: https://www.acq.osd.mil/se/docs/supply-chain-wp.pdf.
39. Rid T., Buchanan B. Attributing Cyber Attacks // The Journal of Strategic Studies. – 2015 – Vol. 38. – Nos. 1-2. – P.4-37. DOI: 10.1080/01402390.2014.977382.
40. Romashkina N.P. New Technologies: Challenges to International Security and Stability // CEUR Workshop Proceedings. Selected Papers of the X Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2019). – 2019. – Vol. 2603. – P.65-69.
41. Stefanovich D. Artificial intelligence advances in Russian strategic weapons // The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Vol. III. South Asian Perspectives. – Stockholm: SIPRI, 2020. – P.25-29. URL: https://www.sipri.org/publications/2020/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-iii-south-asian.
42. Stefanovich D. Proliferation and threats of reconnaissance-strike systems: a Russian perspective // The Nonproliferation Review. – 2020. – Vol. 27. – Issue ½. DOI: 10.1080/10736700.2020.1795370.
43. Stefanovich D. Russia's Basic Principles and the Cyber-Nuclear Nexus // The European Leadership Network. 2020. 14 July. URL: https://www.europeanleadershipnetwork.org/commentary/russias-basic-principles-and-the-cyber-nuclear-nexus/.

ОБ АВТОРАХ

Марков Алексей Сергеевич – профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, доктор технических наук, лауреат премии Правительства в области науки и техники, CISSP, a.markov@bmstu.ru.

Ромашкина Наталия Петровна – руководитель Группы проблем информационной безопасности Центра международной безопасности ИМЭМО РАН им. Е.М. Примакова, член-корреспондент АВН, кандидат политических наук, romachkinan@yandex.ru.

Стефанович Дмитрий Викторович – научный сотрудник Центра международной безопасности ИМЭМО РАН им. Е.М. Примакова, hasstef@gmail.com.

Научное издание

Ромашкина Наталия Петровна
Марков Алексей Сергеевич
Стефанович Дмитрий Викторович

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ, СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Монография

ISBN 978-5-9535-0581-9

Подписано в печать 28.12.2020.
Формат 60×84/8. Печать офсетная.
Объем 12,25 п.л., 5,9 а.л. Тираж 300 экз. Заказ № 41/2020

Издательство ИМЭМО РАН
Адрес: 117997, Москва, Профсоюзная ул., 23