Секция «Конфликты в «цифровом обществе»: природа, специфика, механизмы решения»

Проблемы обеспечения информационной безопасности в киберпространстве

Научный руководитель – Устинкин Сергей Васильевич

Горюнова Анна Андреевна
Аспирант
Нижегородский государственный лингвистический университет им. Н.А. Добролюбова, Нижний Новгород, Россия
E-mail: asukhanova@list.ru

Современная система взглядов политического руководства РФ на информационную безопасность изложена в Доктрине информационной безопасности, утвержденной В.В. Путиным 5 декабря 2016 года [3]. Мощное информационное воздействие на население, зависимость компонентной базы в области производства компьютерного оборудования и программного обеспечения - эти и другие угрозы киберпространства были обозначены в ней как проблемы межгосударственного уровня.

Международный информационный обмен все чаще используется для достижения геополитических, военных, стратегических и экономических целей различных акторов, включая государства, ТНК, международные организации, криминальные и террористические структуры. Информационные войны в киберсреде могут быть отнесены к военным действиям [5]. Существует тонкая грань между вредоносным программным обеспечением и кибероружием, определяемая политическим, юридическим, экономическим контекстом ситуации.

Помимо интернета в киберпространство входят другие сети и системы, например, через которые происходит обмен информацией на биржах, системы управления электронными устройствами через удаленный доступ, системы гражданской и военной связи, а также управление военной и оборонной техникой, такой как беспилотные летательные аппараты, ракеты, боевые роботы. Современное киберпространство представляет собой пятое возможное поле разворачивания военных действий после земли, воды, воздуха и космоса. Понимание разведывательной деятельности вступило в новый этап вскоре после развития киберпространства, что обуславливает необходимость изучения этой сферы в политическом контексте.

Использование новых информационных технологий (ИТ) без систем обеспечения информационной безопасности может привести ко многим проблемам. Помимо экономических целей, увеличиваются масштабы угроз в области обороноспособности страны, которые нацелены на подрыв социальной стабильности государства и его суверенитета. Эксперты отмечают усложнение и увеличение масштабов компьютерных атак, а также усилением деятельности иностранных разведывательных и специальных служб.

Зарубежное исследование о национальной безопасности США, опубликованное в 2019 году, выделяет 4 новейших технологии, оказывающих большое влияние на национальную безопасность страны: искусственный интеллект, машинное обучение, квантовые компьютеры и биотехнологии. Важно отметить, что 3 из этих 4 неразрывно связаны с ИТ. Если в настоящее время полноценно работающие квантовые компьютеры являются гипотетическим устройством, то остальные в разной степени уже применяются как в финансовой, так и в военной сфере. Однако прорыв в любой из этих технологий приведет к резкому устареванию имеющихся технологий и снижению уровня безопасности. Использование искусственного интеллекта уже применяется в аналитических процессах в корпорациях «Google» и «Amazon». Разведывательные и военные службы всего мира исследуют пути использования этой технологии в своих целях [1].

В современном мире именно информационная сфера и киберсреда в состоянии принять на себя роль основных полей противостояния сторон, не допуская перехода конфликта в вооруженную стадию [5]. Анонимность киберпреступлений при проникновении в систему управления хозяйством или военную сферу является фактором повышенной опасности.

В 2007 году применение кибероружия на гражданских ведомствах ощутила на себе Эстония. а в 2009-2010 году произошло вторжение в военный сектор Ирана вирусом Styxnet.

В последнее время в России увеличивается число киберугроз. Согласно лаборатории Касперского, предприятия малого и среднего бизнеса теряют около 780 тыс. руб. от каждой атаки, а при атаке на организации ОПК или военные ведомства существенно возрастают риски. В целях противодействия кибервойнам и киберугрозам необходимо обеспечить более надежную защиту от взломов организаций военного и оборонного секторов [4].

В этих целях в 2016 году госкорпорацией «Ростех» был создан Корпоративный центр обнаружения и ликвидации последствий компьютерных атак (КЦОПЛ). Согласно официальной информации, В 2018 году было проведено таких атак 322, и еще более 1,5 млн. инцидентов разного рода было зафиксировано в сфере информационной безопасности [2]. КЦОПЛ взаимодействует с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Пандемия коронавируса в 2020 году, сопряженная с режимом самоизоляции, используемым во многих странах мира, ускорила процессы перехода многих компаний в киберпространство. Для обеспечения кибербезопасности необходимо создавать собственные программы, и развивать международное сотрудничество в этой сфере. Таким образом, киберпространство расширяет научные, технологические и коммерческие возможности, но и скрывает в себе большие риски, особенно в сфере безопасности.

Источники и литература

1) Alden, E. Technology and National Security: Maintaining America's Edge. Washington, D.C.. The Aspen Institute. 2019
2) https://rostec.ru/news (Официальный сайт Госкорпорации «Ростех»)
3) Доктрина информационной безопасности РФ. Электронный доступ http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (проверено 23.10.2020)
4) Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность. 2018 Электронный доступ https://cyberleninka.ru/article/n/kiberprostranstvo-kak-novaya-politicheskaya-realnost-vyzovy-i-otvety/viewer (проверено 23.10.2020)
5) Перская В.В. Информационное противостояние и киберсреда – основной сегмент противостояния в условиях перехода к многополярности. // Большая Евразия: Развитие, безопасность, сотрудничество. 2019. Электронный доступ https://cyberleninka.ru/article/n/informatsionnoe-protivostoyanie-i-kibersreda-osnovnoy-segment-protivodeystviya-v-usloviyah-perehoda-k-mnogopolyarnosti/viewer (проверено 23.10.2020)