Список источников

1. Арчаков, В. К пониманию феномена современных «сетевых революций» в контексте обеспечения национальной безопасности Республики Беларусь / В. Арчаков, А. Баньковский, Ю. Александров // Беларуская Думка. – 2021. – № 12. – С. 47–57.

2. Мигун, Д. А. Информационный экстремизм и информационная безопасность / Д. А. Мигун. – Минск : РИВШ, 2020. – 64 с.

3. Политические институты и процессы в информационном обществе : учеб. пособие / И. В. Вашкевич [и др.] ; под ред. И. В. Вашкевич. – Минск : БГУИР, 2018. – 236 с.

4. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 года № 1 «О концепции информационной безопасности Республики Беларусь» // Национальный правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P219s0001&ysclid=la29rok0us664497979. – Дата доступа: 04.11.2022.

***А.А. Филон, А.Т. Семенова**, студентки*
Научный руководитель – М.В. Гурина, магистр управления и права
АУпПРБ (Минск)

ИНФОРМАЦИОННЫЕ ВОЙНЫ КАК ИНСТРУМЕНТ СОВРЕМЕННОЙ ПОЛИТИКИ

В современном обществе неприемлемо решение политических или иных проблем при помощи физической силы. Все чаще в качестве инструмента политики используются информационные войны, которые зачастую наносят противнику более негативные последствия, чем физическое насилие.

Информационная война – это действия, предпринимаемые с целью достижения информационного превосходства, воздействия на информацию, информационные процессы и информационные системы противника при одновременной защите информации, информационных процессов и собственных информационных систем. Информационная война основана на использовании информационно-коммуникационных технологий для нанесения ущерба стороне противника.

Существует ряд принципов информационной войны, в полной мере описывающих отличительные черты подобной конфронтации.

Первый принцип – это обезглавливание, который гласит, что командование и управление, системы поддержки принятия решений и взаимодействия должны быть основной целью информационной войны, чтобы изолировать

командование противника от его боевых сил. Также необходимо уничтожить вражеские датчики перед вступлением в бой.

Другой основополагающий принцип – это знание, согласно которому всем, кто нуждается, должно быть доступно как можно больше информации, и что ее распространение должно быть максимально плавным.

Принцип выживания заключается в том, что политика и стратегия должны быть централизованы, а планирование и выполнение, напротив, должны быть децентрализованы, чтобы максимально затруднить нападение противника. Каждый участник должен иметь четкое представление об общей картине задачи, чтобы наилучшим образом способствовать достижению целей, когда будет затронуто центральное командование в своей системе управления и контроля.

Еще одним принципом является интенсивность. Следует прилагать все возможные усилия и избегать политического вмешательства на оперативном уровне. Уязвимости, которые могут быть использованы внутренними или внешними противниками, являются первостепенными объектами, на которые государству необходимо наложить ограничения.

Информационная война включает в себя различные методы. Основной метод работы – это уничтожение информационных систем противника. Например, возможность помешать военной связи или системам связи вооружения противника. Также можно осуществлять атаки, такие как физические или кибератаки, на системы связи государственных служб, например, аэропорты, финансовые рынки, больницы, для вывода из строя инфраструктуры.

Сбор ключевой информации о противнике, его стратегиях и маневрах также является одним из методов информационной войны, в которые входят шпионаж и анализ личных данных. В информационной войне могут использоваться такие инструменты, как бот-сети или фишинговые атаки для выполнения широкого ряда действий от компрометации конфиденциальных компьютерных систем до кражи конфиденциальной информации.

Зачастую участники информационных войн прибегают к такому методу, как нейтрализация определенных средств связи, а именно телевидения, радио, веб-страниц противника. Одна из воюющих сторон может мешать телевизионным трансляциям своего противника или запускать распределенные атаки типа DDoS. DDoS-атаки нацелены на нейтрализацию компьютера, сети или веб-страницы. Они направляют большое количество запросов, что делает их бесполезными.

Наконец, еще одним инструментом выступает распространение неверной информации или пропаганда с целью манипулирования общественным мнением

оппонента. В некоторых случаях злоумышленники взламывают телеканалы или веб-страницы для рассылки дезинформационных сообщений.

Феномен информационной войны имеет глубокие корни. В прошлом пропаганда также использовалась как оружие войны. Не многим известно, что война Германии против СССР началась не 22 июня 1941 года, а намного раньше. Целью информационной войны немцев было ввести в заблуждение советское руководство относительно точной даты своего нападения на СССР. Инициатором начала информационной войны против СССР был А. Гитлер. В конце зимы 1941 года по его указанию была разработана операция по дезинформационному прикрытию подготовки к нападению на СССР. Ее целью было стремление вызвать у советского руководства недоверие к огромному потоку сообщений о предстоящем в ближайшее время военном выступлении Германии против СССР, создать информационный хаос и заставить И. Сталина медлить и не проводить мобилизацию. Вся эта ситуация является хорошим историческим примером рассматриваемой нами проблемы.

Однако сегодня тактике информационной войны придает новую силу использование социальных сетей, посредством которых увеличивается распространение фальшивых новостей и сообщений.

Современные технологии также позволяют создавать более реалистичные фиктивные отчеты благодаря методам, известным как «дипфейки». Например, они дают возможность создания поддельных видео на основе реальных. Хакеры могут приписывать спорные заявления политическим деятелям и распространять поддельное видео, с целью дискредитации. Данный метод использовался в различных случаях, особенно для влияния на выборы в разных странах.

Правительственные организации должны определить конфиденциальную информацию и риски, если она будет скомпрометирована, иначе им не избежать саботажа. Враждебные правительства или террористы могут украсть информацию, уничтожить ее или использовать внутренние угрозы.

Атака на электросеть является одной из самых опасных, так как позволяет злоумышленникам отключить критически важные системы, разрушить инфраструктуру и потенциально нанести телесные повреждения. Атаки на электросеть также могут нарушить связь и ограничить функционирование мессенджеров.

Несомненно, не только с проявлениями информационной войны, но даже с попытками ее реализации необходимо вести борьбу. Правовой статус этой новой области до сих пор неясен, поскольку не существует международного права, регулирующего использование кибероружия. Однако это не означает, что кибервойна не регулируется законом. В Республике Беларусь существует Концепция национальной безопасности Республики Беларусь, отражающая национальные интересы, внутренние и внешние источники угрозы. Данная

концепция распространяется на множество сфер общественной жизни, в частности и на информационную.

Лучший способ оценить готовность страны к кибервойне – это провести учение или симуляцию в реальной жизни, также известную как военная игра в киберпространстве. Военная игра позволяет проверить, как правительства и частные организации реагируют на сценарий кибервойны, выявить недостатки в защите и улучшить взаимодействие между организациями. Военная игра может помочь защитникам научиться действовать быстро при защите критически важной инфраструктуры и спасти жизни, потому необходимо принять некоторые меры, чтобы обезопасить себя и свою страну в будущем, ведь неизвестно, с какими трудностями нам еще предстоит встретиться.

Список источников

1. Кихтан, В. В. Информационная война: понятие, содержание и основные формы проявления / В. В. Китхан, З. Н. Качмазова // Вестник Волжского университета имени В.Н. Татищева. – 2018. – Т. 2, № 2. – С. 228–235.

2. Вирен, Г. Современные медиа: Приемы информационных войн / Г. Вирен. – М. : Аспект Пресс, 2013. – 126 с.

3. Хомков, А. В. Методы и цели информационных войн [Электронный ресурс] / А. В. Хомков. – Режим доступа: https://scienceforum.ru/2016/article/2016023722. – Дата доступа: 19.11.2022.