КИБЕРБЕЗОПАСНОСТЬ КАК ЧАСТЬ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В УСЛОВИЯХ СОВРЕМЕННЫХ ВЫЗОВОВ И УГРОЗ

Д.Н. Николичев, А.М. Фёдорова

Ключевые слова: кибербезопасность, киберугроза, интернет, кибератака.

Кибербезопасность как часть комплексной безопасности государства в условиях современных вызовов и угроз, является одной из главных задач любого суверенного государства, не исключая и Республику Беларусь.

Современный этап общемирового развития уходит из реального мира в информационную сферу, и в связи с этим и появилась необходимость в «безопасном интернете». Превращаясь в системообразующий фактор жизни общества, она все более активно влияет на состояние политической, экономической, оборонной, личной, имущественной и других составляющих безопасности. Информационная сфера является психологическим рычагом воздействия на людей.

Целью данной статьи является анализ кибербезопасности как части комплексной безопасности государства в условиях современных вызовов и угроз.

Материал и методы. Теоретическую основу составили труды Алпеева А.С., Ромашкина Н.П., Петрова В.П. В ходе исследования применялись общенаучные методы индукции и анализа. Также был использован специальный метод – формально-юридический.

Результаты и их обсуждения. Первая стратегия кибербезопасности появилась в 2003 году в США [4, с. 78]. После чего подобные стратегии и планы мероприятий по безопасности в виртуальном пространстве распространились по всей Европе.

Есть множество определений термину «кибербезопасность». Например, Постановление Совета Безопасности Республики Беларусь № 1 «О Концепции информационной безопасности Республики Беларусь» определяет:

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз [2].

Как считает к.т.н. Алпеев А.С. кибербезопасность – раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов, с целью выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности [1, с. 37].

Таким образом, в связи с переходом мировой экономики и других сфер на цифровое поле возникает необходимость в осуществлении мер

безопасности этого поля. В связи с этим и по сей день разрабатываются и совершенствуются мероприятия по осуществлению безопасного использования цифрового пространства.

Как и было описано выше, ссылаясь на официальный источник и научную точку зрения, понятие кибербезопасности можно определить следующим образом: это отдельное направление сферы обеспечения безопасности, действующее в границах цифрового пространства и осуществляющая деятельность по предупреждению и исключению цифровых угроз (киберугроз) любых уровней, независимо от сферы обслуживания.

На безопасное функционирование информационных систем влияют такие факторы: интернет атаки, выход из строя программного и аппаратного обеспечения, человеческий фактор и др.

Сложность сдерживания потенциальных и реальных «киберугроз» относится к числу наиболее важных проблем национальной безопасности государств. Современное общество зависит от стабильной работы информационных систем. Нынешние реалии показывают, что хищение информации юридического лица любой организационно-правовой формы, такой как персональных данных, секреты производства (ноу-хау), различныхтехнологий выполнения работ и/или оказания услуг. Всё это оказывает пагубное влияние на развитие экономики как предприятия, так и в дальнейшем экономики целой страны.

Проблемы защиты информации волновали людей с древних времён, ещё в VI веке до нашей эры китайский военачальник Сунь-Цзы «изложил ряд информационно-интеллектуальных приёмов ведения военных действий» [3, с. 54], в XVI веке философ Н. Макиавелли «сформулировал информационно-психологическую концепцию, где изложил принципы внедрения информационного противоборства в политической сфере» [3, с. 55]. История знает множество примеров информационно-пропагандистских акций, основанных на дезинформации и утечке данных.

Кибербезопасность информационных систем затрагивает все слои населения и сферы деятельности человека. В нынешнее время кибератаки является частью информационных войн, а глобальная сеть интернет – распространяя ложную информацию («фэйки»). Пользователь, посредством различных мессенджеров, чатов, имеет возможность быть «анонимным куратором», координируя действия, управляя группой людей, действуя радикально и деструктивно мысля в отношении реализации провокаций, террористических актов, госпереворотов и других не правомерных деяний, а так же втягивания молодого поколения, вербуя их в экстремистские организации.

Наши предприятия зачастую используют компьютерные технологии и информационные системы, с каждым годом это зависимость возрастает (для продвижения предприятия, товаров, услуг), и в случае кибератаки при помощи вредоносных программ и других методов, могут «парализовать» предприятия, блокировать официальные сайты – это может сказываться на

психологическом климате населения, вызвать панику. Уязвимость информационных коммуникаций при кибератаках может подвергнуть экономику, национальную обороноспособность, политическую стабильность к спаду, без использования огневой мощи либо военных действий.

Заключение. Наиболее серьезными киберугрозами безопасности и стабильности являются применение информационных систем в военно-политических целях («гибридная война») для осуществления агрессивных действий, актов агрессии; снижение общественной стабильности, разжигание межэтнической, межнациональной розни посредством информационных систем вмешательство во внутренние дела суверенного государства, деструктивное кибервоздействие на объекты критически важной государственной инфраструктуры. Международное нормативно-правовое управление в этой области пока отсутствует. При этом ситуация, связанная с обеспечением необходимого и достаточного уровня стратегической стабильности, сегодня может оцениваться как кризисная.

Список использованных источников

1. Алпеев А.С. Терминология безопасности: Кибербезопасность, Информационная безопасность. Журнал «Вопросы кибербезопасности». 2015. № 5. 36-42 с.

2. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. – Минск,2022.

3. Петров В.П., Петров С.В. Информационная безопасность человека и общества: учебное пособие / В. П. Петров, С. В. Петров – М. : Изд-во НЦ ЭНАС, 2007. – 336 с.

4. Ромашкина Н.П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. № 5. 77-86 с.

СТАНОВЛЕНИЕ СУДЕБНОЙ СИСТЕМЫ В ПЕРВЫЕ ГОДЫ СОВЕТСКОЙ ВЛАСТИ

А.П. Петров, В.А. Петров

Ключевые слова: юстиция, суд, правосудие, трибунал, защита.

После Октябрьской революции вся дореволюционная система судов была сломлена. Перед молодой Советской властью стал вопрос об организации ново судебной системы, которая отвечала бы требованием времени.

Цель – показать становление судебной системы в первые годы советской власти.

Материал и методы. Научную теоритетико-правовую базу исследования составили декреты Советской власти за период с 25 октября 1917 года по ноябрь 1920 года, закреплявшие судебную систему, порядок ее организации и рассмотрения гражданских и уголовных дел.

В качестве методов исследования использовались системный анализ, логически, исторический анализ, сравнительного правоведение.