ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

Вавринович А.Р.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лагунова Е.Н. – преподаватель

Аннотация. В работе рассматривается понятие безопасности в контексте развития информационных технологий и цифровизации общества.

На рубеже XX и XXI веков произошли существенные изменения в обществе, связанные с ростом влияния информации и информационных технологий (ИТ) на различные аспекты жизни человека. Информационная сфера приобретает ключевое значение для современного общества и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы. Развивается информационное взаимодействие, образовываются сетевые сообщества для обмена информацией, опытом и знаниями. Роль ИТ в реализации прав и свобод граждан значительно возросла. Вместе с тем трансформация социума в информационное общество создала новые риски и угрозы, затрагивающие вопросы национальных и международных аспектов обеспечения информационной безопасности. Основной составляющей термина «информационная безопасность» является само понятие безопасности, которое подразумевает наличие не только технологических, но и политико-идеологических угроз в данной области.

Поддержание информационной безопасности – необходимое условие нормального развития международных отношений в сфере информационного обмена и использования киберпространства, обеспечения прав и свобод граждан, юридических лиц, а также национальной безопасности государств в информационной сфере.

Вопросы обеспечения международной информационной безопасности занимают важное место в повестке дня Генеральной Ассамблеи ООН и других международных организаций. В 1998 году Генеральная Ассамблея ООН приняла резолюцию «Достижения в сфере информатизации и телекоммуникаций», в которой впервые была сформулирована «триада угроз информационной безопасности»: использование ИТ в военно-политических целях; использование ИТ в преступных целях; использование ИТ в террористических целях.

Главными угрозами международной информационной безопасности является военно-политическое использование ИТ. К таким угрозам относится использование ИТ для деструктивного воздействия на личность, общество и государство, с целью разжигания межнациональной и межконфессиональной вражды, формирования радикального и протестного потенциала, подрыва суверенитета государств, вмешательства в их внутренние дела, нарушения их территориальной целостности, путем подготовки и проведения информационных операций и войн. Многие государства осуществляют мероприятия по формированию как оборонительного, так и наступательного информационного потенциала. К этому виду угроз также относится получение несанкционированного доступа к государственной тайне и другой конфиденциальной информации, раскрытие которой может нанести ущерб интересам государства. Возрастает число случаев использования ИТ для шпионажа и распространения вредоносных программ, направленных на получение доступа к системам управления стратегическими объектами различных инфраструктур (военных, промышленных и др.). Современные вооруженные конфликты все чаще переносятся в цифровое пространство, где достижение целей осуществляется не только уничтожением вооруженных сил противника, но и подавлением его систем государственного и военного управления.

К преступным угрозам относятся: неправомерная деятельность в отношении цифровой информации, включая персональные данные; создание и распространение вредоносных программ; осуществление мошеннических операций с использованием ИТ; получение неправомерного доступа к финансовой, банковской и другой информации и использование ее в корыстных целях; распространение неправомерной информации с целью вовлечения в приступную деятельность; использование ИТ для обеспечение преступной деятельности; реабилитация нацизма, оправдание геноцида и преступлений против мира и человечности; нарушение авторских и смежных прав. В настоящее время предотвращение таких видов преступлений против общества и государства является одной из ключевых задач национальной политики безопасности.

Терроризм является одним из самых серьезных вызовов мировому сообществу. К террористическим угрозам относится использование ИТ в качестве инструмента для пропаганды идеологии терроризма, совершения атак на информационные системы, обеспечения террористической деятельности (организация и планирование терактов, сбор финансовых средств и т.д.). Противодействие терроризму становится ключевой задачей как национальной, так и международной безопасности.

Защищенность национальных интересов государств – это основная задача в области информационной безопасности, обеспечение которой предполагает реализацию комплекса правовых, организационных, технологических и кадровых мероприятий.

В силу ряда причин политического, экономического и исторического характера национальные интересы государств-членов международного сообщества могут не совпадать, что создает предпосылки к формированию государствами своих национальных систем обеспечения информационной безопасности. В то же время глобальность процессов информационного взаимодействия в международном сообществе, трансграничность компьютерной преступности делают необходимым объединение усилий различных государств по обеспечению информационной безопасности международного сообщества в целом.

Меры по обеспечению информационной безопасности включают следующие аспекты:

1) Разработка международным сообществом согласованных стратегий в области обеспечения информационной безопасности, контроля за производством и распространением информационного оружия, координации деятельности в борьбе с кибертерроризмом и международными компьютерными преступлениями, защиты интеллектуальной собственности и авторских прав на материалы, распространяемые в открытом доступе, разработка систем противодействия этим угрозам.

2) Интеграция государств-членов международного сообщества в систему международной информационной безопасности, повышение концептуальной и технологической совместимости, синхронизация целей и задач национальных систем обеспечения информационной безопасности с системами других государств и организаций.

3) Совершенствование нормативно-правовой базы в области обеспечения прав и свобод граждан в информационной сфере, включая правовые нормы, регулирующие отношения в области массовой информации.

4) Развитие национальных систем подготовки кадров в области информационной безопасности и ИТ.

5) Укрепление взаимодействия правоохранительных органов государств-членов международного сообщества для предотвращения компьютерных преступлений и применения юридической ответственности.

Координация международного сотрудничества в вопросах информационной безопасности осуществляется различными органами, такими как Генеральная Ассамблея ООН, НАТО, Совет коллективной безопасности ОДКБ и другие специализированные структуры. Между тем сотрудничество, направленное на консолидацию глобального взаимодействия в этой области, имеет множество проблем, основной причиной которых является противоборство между ведущими мировыми центрами силы. На данный момент отсутствуют комплексные международные договоры универсального характера, регулирующие сотрудничество государств в области международной информационной безопасности и борьбы с преступностью в сфере ИТ. Тем не менее, киберпространство не является средой «вне закона», на него распространяются общепризнанные принципы международного права.

Беларусь уделяет большое внимание вопросам информационной безопасности. В 2019 году была утверждена «Концепция информационной безопасности Беларуси», которая провозгласила информационный суверенитет, уважение цифрового суверенитета других стран и проведение мирной внешней информационной политики.

Беларусь активно развивает сотрудничество в области международной информационной безопасности, противодействия киберпреступности и терроризму, для чего активно принимает участие в конференциях ООН по данным вопросам, в заседаниях Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Беларусь также является соавтором резолюции Генеральной Ассамблеи ООН 75/282 «О противодействии использованию информационных и коммуникационных технологий в преступных целях», которая определила модальности работы специального комитета для разработки универсальной международной конвенции по борьбе с использованием ИТ в преступных целях.

Список использованных источников:

1. Концепции информационной безопасности Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.mogileviro.by/wp-content/uploads/2022/10/13-18-03-2019_1-ucx.pdf – Дата доступа 27.03.2024.

2. Проблемы информационной безопасности в современном мире [Электронный ресурс]. – Режим доступа: https://studylib.ru/doc/2258340/problemy-informacionnoj-bezopasnosti-v-sovremennom-mire – Дата доступа 27.03.2024.

3. Министерство иностранных дел Республики Беларусь. Международная информационная безопасность [Электронный ресурс]. – Режим доступа: https://www.mfa.gov.by/mulateral/global_issues/inform/ – Дата доступа 27.03.2024.

4. Международно-правовые основы обеспечения международной информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/345986009_MEZDUNARODNO-PRAVOVYE_OSNOVY_OBESPECENIA_MEZDUNARODNOJ_INFORMACIONNOJ_BEZOPASNOSTI – Дата доступа 27.03.2024.