правоохранительных органов и обеспечить более высокий уровень общественной безопасности.

Минаев В.А.,

доктор технических наук, профессор
Московский университет МВД России имени В.Я. Кикотя

Кибербезопасность современных систем

Руководствуясь концепцией своего развития, Россия активно формирует архитектонику интернет-державы, запрягши трех современных цивилизационных коней: стимулирование цифровой экономики, формирование чистой и надежной онлайн-среды, обеспечение безопасности киберпространства[1].

В рамках построения названной архитектоники страна постоянно повышает охват широкополосным доступом в Интернет во всех своих регионах, включая северные и дальневосточные территории с низкой плотностью населения. Россия наращивает сотрудничество со многими другими государствами при создании безопасного и устойчивого киберпространства.

В этой связи Президент Российской Федерации В.В. Путин неоднократно призывал все мировое сообщество к сотрудничеству в сфере Интернета и цифровой экономики.

Создается цифровая Россия, нацеленная на глубокое слияние Интернета, технологий Big Data, искусственного интеллекта и реального сектора экономики. Перспективы реализации этих фундаментальных планов – это начало развития территорий, поселений и отдельных индивидов, по сути дела, с «цивилизационного нуля». Это фактически означает, что на современном этапе ни один человек в стране и ни одна страна в мире уже не смогут обходиться в своей жизнедеятельности без сетевого пространства, которое предстоит строить совместно. По отдельности – никак не получится, поскольку масштабы, которые несет новая техническая революция, превышают все аналоги прошлого.

Характерно на этот счет мнение руководителя компании «Лаборатория Касперского»[2], который сказал, что человечество живет в очень опасном мире, и оно сегодня уязвимо как никогда. Если в 1997 г., по его словам,

[1] Подр.: Минаев В.А., Поликарпов Е.С. Китайский взгляд на развитие и безопасность киберпространства // Информация и безопасность. 2023. Т. 26. Вып. 4. С. 535-542.

[2] Касперский заявил о появлении 90 млн новых вирусов за год. URL: https://www.rbc.ru/technology_and_media/03/12/2017/5a2405079a7947213b28 a893. (дата обращения: 28.11.2024).

существовало полтысячи вредоносных программ и вирусов, то сейчас их насчитывается более 20 млн. Появился даже новый тренд – многослойность и многоуровневость в разработке и реализации вредоносных программ.

Информационные войны, фейковая информация как их отражение в различных форматах и представлениях все более увеличивают свою масштабность на фоне разрастающихся конфликтов в разных регионах мира.

Нестабильность в киберпространстве обостряет глобальные проблемы, усиливает турбулентность в современных международных отношениях. Во многом это обострение связано с попытками кибергегемонизма в информационной сфере, усилением информационного деструктивного воздействия на население, масштабных злоупотреблений с данными в цифровой сфере. Все это требует повышения эффективности управления киберпространством на основе сетецентрических технологий[1].

Ключевые направления формирования единого киберсообщества:

– активное содействие цифровой индустриализации и цифровой трансформации общества, связанным с созданием глобальной информационной инфраструктуры, включая обеспечение всех регионов доступными интернет-услугами;

– развитие сообщества безопасности киберпространства на основе соблюдения принципов нейтральности информационных технологий, оперативного обмена данными о киберугрозах, трансграничной координации по противодействию киберэкстремизму и кибертерроризму;

– формирование коллективной киберответственности, позволяющей органам власти, силовым структурам, интернет-компаниям, бизнес-сообществам, общественным организациям способствовать созданию адекватных норм управления киберпространством страны;

– гармонизация киберинтересов государства, его регионов и социальных групп. Это означает создание киберпространства, в котором на первом месте стоит человек с его цифровыми интересами и интернет-культурой.

Рассмотрим четыре основных принципа, которым необходимо следовать при создании единого киберпространства:

– соблюдение цифрового суверенитета, постулирующего право государств выбирать собственные пути развития Сети и модели равноправного участия в международном управлении киберпространством;

– формирование устойчивости и безопасности киберпространства как фактора предотвращения в нем криминальных действий и агрессии, экстремизма и терроризма, незаконного оборота наркотиков и других запрещенных объектов;

[1] Научно-технологический прогресс в современных международных отношениях : учебник для вузов: в 2 т. / под общ. ред. А.В. Бирюкова. М.: Аспект Пресс, 2023. Т. 1. 368 с.

– содействие открытости и сотрудничеству как предпосылки проведения транспарентной политики в киберпространстве, создания платформ эффективного сотрудничества в нем, координации инноваций;

– поддержание киберпорядка, выражающегося в руководящей роли нравственного воспитания и достижений человеческой цивилизации.

Очищение цифрового контента.

Российское общество следит, чтобы в Интернете обеспечивалась безопасность, выступающая многомерным объектом, которому присущи:

– позитивная энергия в Сети, где возрастает масса позитивного и здорового контента, передовые культурные элементы;

– разнообразие цифровой культуры, представленной видео- и аудиоматериалами, литературой, музыкой, электронными библиотеками, музеями в облачных хранилищах, онлайн-театрами, выставками и концертами;

– передовые средства онлайн-коммуникации и обработки данных, включающие методы искусственного интеллекта, технологии больших данных, облачные вычисления, виртуальную и дополненную реальность;

– киберэкосистемные представления об Интернете, направленные на обеспечение чистой и здоровой киберсреды, очищенной от противоправного и аморального контента;

– продвижение интернет-цивилизации, включающее создание здорового сообщества в Сети, формирование праведной интернет-культуры;

– развитие работы онлайн-платформ, содействующих качественному социально-экономическому развитию и устремлениям людей к лучшим образцам жизни.

С целью укрепления рубежей своего киберпространства в России создается фундаментальная нормативная правовая база, включающая в первую очередь законодательство о кибербезопасности, безопасности данных и защите персональных данных. В частности, в стране разработана нормативная база о безопасности и защите критической информационной инфраструктуры (КИИ), усилена работа в области оценки рисков, надзора и раннего предупреждения чрезвычайных ситуаций.

Огромное влияние на комплексное обеспечение безопасности киберпространства России оказывает обучение в десятках ее учебных заведений кибербезопасности как основной дисциплине. При этом все в большей мере концепция преподавания и опережающей подготовки кадров в области основ кибербезопасности опирается на схему, представленную на рисунке 1.

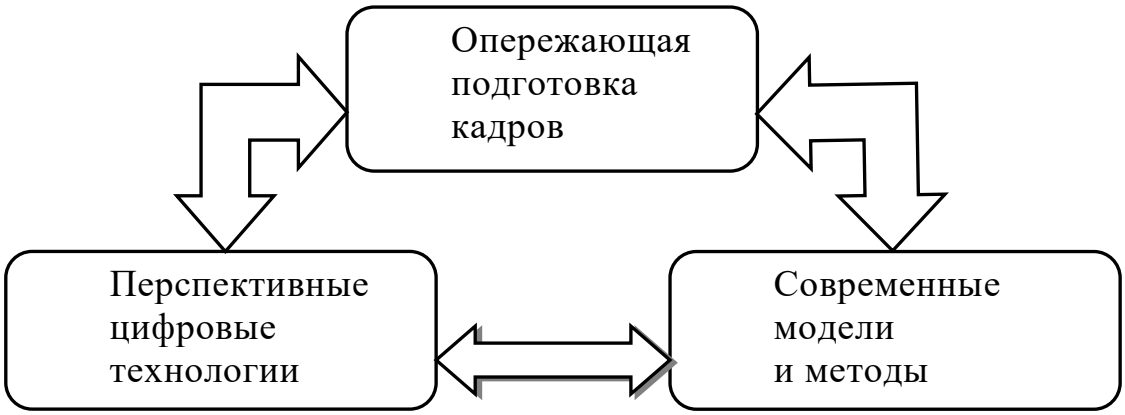

Рис. 1. Концепция преподавания и опережающей подготовки кадров
в области основ кибербезопасности

Одновременно поощряются инновационные структуры в области кибербезопасности, создаются национальные парки и пилотные зоны кибербезопасности.

Чтобы в целом охарактеризовать подход Российской Федерации к системному созданию единого киберпространств, кратко охарактеризуем ее усилия в этой сфере, выделив десять направлений.

1. Цифровой суверенитет, смысл которого состоит в праве каждой страны самостоятельно выбирать свой путь цифрового развития, модель и государственную политику управления Сетью при равных возможностях.

2. Поддержание безопасности и стабильности, содержание которых состоит в интеграции интересов всех стран и устранении ситуаций, когда безопасность одних обеспечивается за счет других.

3. Создание недискриминационной цифровой среды, означающей устранение политизации технологических процессов, поддержание безопасных и стабильных цепочек поставок ИТ-продуктов и услуг, а также разработку международных правил управления цифровыми технологиями.

4. Укрепление защиты КИИ как основы нормального функционирования экономики и общества путем взаимного раннего предупреждения о чрезвычайных ситуациях в информационной сфере.

5. Безопасность и стабильность системы управления ресурсами Интернета, гарантирующие их доступность и надежность.

6. Противодействие киберпреступности и кибертерроризму как глобальному бедствию[1].

[1] Подр.: Минаев В.А., Поликарпов Е.С., Симонов А.В. Методы снижения шумовых факторов при выявлении контента экстремистского характера в социальных медиа // Информация и безопасность. 2022. Т. 25. Вып. 2. С. 179-186; Минаев В.А., Симонов А.В. Сравнение моделей-трансформеров BERT при выявлении деструктивного контента в социальных медиа // Информация и безопасность. 2022. Т. 25. Вып. 3. С. 341-348.

7. Безопасность, развитие и использование данных как основы цифровых, интернет- и смарт-технологий[1].

8. Справедливая и рациональная система управления киберпространством, направленного на достижение сбалансированного отражения интересов всех стран-участников.

9. Создание интернет-цивилизации как ключевого объекта в системе прогрессивного развития человечества.

10. Совместное построение и развитие инфраструктуры Интернета для цифрового разрыва между странами и различными социальными группами населения, усиление цифровой помощи его уязвимым слоям.

Орлова Д.Е., Рябчикова Е.А.

Воронежский институт ФСИН России

Обеспечение безопасности телекоммуникационных систем

Распространение телекоммуникационных систем усугубило проблему их безопасности, особенно в отношении защиты передаваемой информации. Утечка ценной информации, например финансовой, может привести к катастрофическим последствиям для владельцев. Из-за стремительного роста ИТ появляются следующие проблемы с информационной безопасностью: использование общедоступных почтовых доменов, недостаточное антивирусное обеспечение и низкая культура ИБ. Помимо этого, угрозы могут исходить от устаревших технологий. Поэтому главной задачей становится надежная защита передаваемых данных, а не только качество и скорость передачи.

При создании новых сетей важно использовать передовые IT-решения для обеспечения необходимого уровня защиты. Защита информации включает комплекс мер против хищения данных, что решается через внедрение норм, таких как ГОСТ-Р 50922-96. Однако развитие технологий требует постоянного совершенствования методов защиты от хакерских атак и обновления стандартов.

Нарушения конфиденциальности и целостности информации могут привести к серьезным последствиям. Ущерб чаще всего связан с утечкой данных, предназначенных для ограниченного круга лиц. Поэтому обеспечение безопасности включает использование надежных технических средств, антивирусов и квалифицированного персонала.

[1] Подр.: Управление информационной безопасностью : учебное пособие / В.А. Минаев, Е.С. Поликарпов, В.Т. Еременко, М.Ю. Рытов. М.: МосУ МВД России имени В.Я. Кикотя, 2022. 310 с.