ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ГОСУДАРСТВЕННАЯ ПОЛИТИКА РЕСПУБЛИКИ УЗБЕКИСТАН

Кучкаров Собир
Преподаватель информатики и информационных технологий,Техникум № 1 Жондорского района Бухарской области

Аннотация: *В статье представлены теоретические основы информационной безопасности, проанализированы современные киберугрозы и раскрыты подходы к их нейтрализации в условиях цифровой трансформации. Особое внимание уделено государственной политике Республики Узбекистан в сфере кибербезопасности, включая актуальные указы и постановления Президента, направленные на формирование устойчивой системы защиты национального информационного пространства.*

Ключевые слова: *информационная безопасность, кибербезопасность, цифровая экономика, защита информации, киберугрозы, государственная политика, цифровизация.*

Современное общество развивается в условиях интенсивной цифровизации, которая охватывает все сферы жизнедеятельности. Информационные ресурсы становятся стратегическим фактором развития государства, а их защита - приоритетной задачей. Увеличение количества кибератак, утечек данных и иных угроз требует формирования эффективной системы информационной безопасности, основанной на научных подходах и поддерживаемой государственными механизмами регулирования. Информационная безопасность представляет собой состояние защищённости информации и информационных систем от внутренних и внешних угроз, обеспечивающее сохранение конфиденциальности, целостности и доступности данных. Данные принципы являются фундаментальными и определяют направления развития современных систем защиты.Цифровая трансформация приводит к усложнению киберугроз, которые становятся более масштабными и технологически продвинутыми. Распространение вредоносного программного обеспечения, целевые атаки на государственные информационные ресурсы, фишинг и социальная инженерия свидетельствуют о необходимости комплексного подхода к обеспечению безопасности. Важным аспектом становится учет человеческого фактора, поскольку именно пользователь зачастую является уязвимым звеном в системе защиты.

Современная модель информационной безопасности основывается на интеграции технических, организационных и правовых механизмов. Технические средства включают криптографическую защиту, системы

мониторинга и предотвращения вторжений. Организационные меры направлены на разработку политики безопасности, управление доступом и оценку рисков. Правовое обеспечение формирует нормативную базу, регулирующую отношения в сфере защиты информации и устанавливающую ответственность за нарушения.В Республике Узбекистан развитие кибербезопасности закреплено на уровне государственной политики. В частности, Указ Президента Республики Узбекистан № УП-6079 от 5 октября 2020 года Стратегия “Цифровой Узбекистан - 2030” определяет кибербезопасность как ключевой элемент цифровой экономики. Документ предусматривает развитие инфраструктуры защиты информации, внедрение современных технологий и подготовку высококвалифицированных специалистов.Дополнительное значение имеют меры, предусмотренные постановлениями Президента, направленные на совершенствование системы кибербезопасности, защиту критической информационной инфраструктуры и развитие национальных центров реагирования на киберинциденты. Новые инициативы ориентированы на переход к проактивной модели обеспечения безопасности, предусматривающей предупреждение угроз и повышение устойчивости информационных систем.

В условиях глобализации особую актуальность приобретает международное сотрудничество в сфере кибербезопасности. Киберугрозы носят трансграничный характер, что требует координации усилий государств и внедрения международных стандартов, включая ISO/IEC 27001. Использование инновационных технологий, таких как искусственный интеллект и анализ больших данных, способствует повышению эффективности систем защиты информации.

Кибербезопасность представляет собой ключевое направление современной информационная безопасность, охватывающее совокупность методов, технологий и организационных мер, направленных на защиту информационных ресурсов, компьютерных систем и сетевой инфраструктуры от внутренних и внешних угроз. В условиях глобальной цифровизации, когда данные становятся стратегическим ресурсом, обеспечение их безопасности приобретает не только техническое, но и социально-экономическое и политическое значение.

Современная киберсреда характеризуется высокой степенью уязвимости, что обусловлено широким распространением интернета, мобильных устройств и облачных технологий. Основу кибербезопасности составляют принципы конфиденциальности, целостности и доступности информации (CIA-триада). Конфиденциальность предполагает ограничение доступа к данным для неавторизованных пользователей, целостность гарантирует неизменность и достоверность информации, а доступность обеспечивает своевременный доступ к ресурсам для легитимных пользователей.Среди актуальных угроз особое место

занимают вредоносные программы (malware), включая вирусы, черви, троянские программы и программы-вымогатели (ransomware), а также атаки, основанные на методах социальной инженерии. Наиболее распространённым примером является фишинг, при котором злоумышленники, маскируясь под надёжные источники, получают доступ к персональным данным пользователей. Также широко распространены атаки типа отказа в обслуживании (DDoS), направленные на перегрузку серверов и нарушение их функционирования.Существенную роль в обеспечении кибербезопасности играет использование криптографических методов защиты информации, таких как шифрование, электронная цифровая подпись и аутентификация. Эти технологии позволяют предотвратить несанкционированный доступ и обеспечить защиту данных при их передаче по открытым каналам связи. Наряду с этим, важное значение имеют системы обнаружения вторжений (IDS/IPS), межсетевые экраны (firewalls), а также регулярное обновление программного обеспечения и управление уязвимостями.Организационные меры также являются неотъемлемой частью комплексной системы киберзащиты. К ним относятся разработка политики информационной безопасности, проведение аудитов, обучение персонала, а также внедрение стандартов и международных практик в области защиты информации. Особое внимание уделяется формированию культуры кибербезопасности среди пользователей, поскольку человеческий фактор остаётся одним из наиболее уязвимых элементов системы.На государственном уровне вопросы кибербезопасности приобретают стратегическое значение. В Узбекистан реализуются программы цифровой трансформации, сопровождающиеся усилением мер по защите национального информационного пространства. Принимаются нормативно-правовые акты, направленные на развитие системы кибербезопасности, создаются специализированные структуры и центры мониторинга киберугроз, а также совершенствуется система подготовки квалифицированных кадров в данной области.Кроме того, кибербезопасность тесно связана с такими направлениями, как защита критической информационной инфраструктуры, безопасность электронного правительства, финансовых систем и персональных данных граждан. Развитие технологий искусственного интеллекта и интернета вещей (IoT) открывает новые возможности, но одновременно порождает дополнительные риски, требующие внедрения более сложных и адаптивных методов защиты.Таким образом, кибербезопасность является многогранной и динамично развивающейся областью, требующей интеграции технических решений, правового регулирования и образовательных инициатив. Эффективная защита в киберпространстве возможна только при условии системного и междисциплинарного подхода, учитывающего как современные угрозы, так и перспективы технологического развития.

Заключение. Информационная безопасность является ключевым фактором устойчивого развития современного общества и государства. Усложнение киберугроз требует формирования комплексной системы защиты, объединяющей научные подходы, современные технологии и государственную поддержку. Реализация стратегических инициатив Президента Республики Узбекистан создает прочную основу для обеспечения безопасности национального информационного пространства и дальнейшего развития цифровой экономики.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Указ Президента Республики Узбекистан № УП-6079 от 5 октября 2020 года «О стратегии “Цифровой Узбекистан – 2030”».
2. Постановление Президента Республики Узбекистан № ПП-3832 от 3 июля 2018 года «О мерах по развитию цифровой экономики».
3. Закон Республики Узбекистан «Об информатизации».
4. ISO/IEC 27001:2013 — Information Security Management Systems.
5. Stallings W. Cryptography and Network Security. — Pearson, 2020.
6. Schneier B. Applied Cryptography. — Wiley, 2019.