Кушнир Светлана Ивановна
канд. ист. наук, доцент, доцент
ФКОУ ВО «Воронежский институт Федеральной
службы исполнения наказаний»
г. Воронеж, Воронежская область
Кушнир Михаил Станиславович
студент
ФГБОУ ВО «Воронежский государственный
университет инженерных технологий»
г. Воронеж, Воронежская область

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР УСТОЙЧИВОГО РАЗВИТИЯ РЕГИОНОВ РОССИИ

Аннотация*: информационная безопасность является одним из ключевых факторов успешного развития современных российских регионов, так как позволяет уменьшить риски, связанные с защитой информации в сфере экономики, политики, социальном развитии, а также предотвратить возможные угрозы от потерь в цифровой сфере.*

Ключевые слова*: информационная безопасность, развитие регионов, экономическое развитие, персональные данные, цифровая экономика, киберпреступность.*

Процесс устойчивого развития российских регионов в трансформационную эпоху представляет собой процесс постоянного улучшения экономических, социальных, культурных и экологических аспектов жизни в регионах России в условиях быстрых изменений и нововведений. Он включает в себя экономическое обновление, социальное развитие, экологическую устойчивость, культурное процветание, технологические инновации.

В эпоху трансформации, когда технологии и глобальные тренды меняют общество и экономику, устойчивое развитие помогает регионам адаптироваться

к этим изменениям, сохраняя при этом баланс между потребностями текущего и будущих поколений.

Факторы устойчивого развития современных российских регионов включают в себя: экономическую стабильность, когда происходит развитие экономики, привлечение инвестиций и создание благоприятных условий для бизнеса; социальную справедливость, т.е. происходит обеспечение равного доступа к образованию, здравоохранению и социальной защите; экологическую устойчивость – защиту окружающей среды, рациональное использование природных ресурсов и снижение загрязнения; технологическое развитие – внедрение инноваций и современных технологий для повышения эффективности и конкурентоспособности; политическую стабильность – создание прозрачных и эффективных государственных институтов и правовой системы; культурное разнообразие – сохранение и развитие культурного наследия и поддержку культурного многообразия [1].

Эти факторы в совокупности способствуют созданию устойчивого и гармоничного развития регионов, который является основой для долгосрочного процветания и благополучия.

Но еще одним важнейшим фактором стабильного развития регионов является Информационная безопасность. Она обеспечивает защиту данных, инфраструктуры и информационных технологий.

Понятие «Информационной безопасности» возникло в конце 20 века, когда компьютерные технологии и глобальные сети стали неотъемлемой частью жизни общества. Информационная безопасность (ИБ) – это комплекс мер, направленных на защиту информации от несанкционированного доступа, использования, изменения, искажения или уничтожения. Это понятие возникло в контексте быстрого развития информационных технологий и глобальных компьютерных сетей, таких как Интернет. Её суть заключается в защите информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, изменения, проверки или уничтожения [2].

Приведем лишь некоторые аспекты информационной безопасности, подчеркивающие её значение:

1) защита критически важной инфраструктуры – регионы зависят от информационных систем для управления энергетикой, транспортом и другими жизненно важными функциями. Информационная безопасность помогает предотвратить сбои и атаки, которые могут привести к серьёзным последствиям;

2) экономическая стабильность – безопасность данных способствует доверию инвесторов и потребителей, что важно для привлечения бизнеса и поддержания экономической стабильности;

3) защита персональных данных – с учётом роста цифровой экономики и онлайн-сервисов, защита личной информации становится всё более важной для сохранения прав и свобод граждан;

4) противодействие киберпреступности – развитие информационной безопасности помогает бороться с киберпреступностью, которая может нанести ущерб экономике и безопасности региона.

Сотрудники, деятельность которых связана с обеспечением информационной безопасности, проводят ряд мероприятий для обеспечения устойчивого развития российских регионов. Вот некоторые примеры таких мероприятий:

Разработка и внедрение политик безопасности – создание строгих правил и процедур для защиты информационных ресурсов и инфраструктуры.

Обучение и повышение осведомленности сотрудников – регулярное проведение тренингов и семинаров по информационной безопасности для сотрудников всех уровней.

Аудит и мониторинг систем – проведение регулярных проверок и мониторинга информационных систем на предмет уязвимостей и атак.

Инцидентный менеджмент – разработка процедур быстрого реагирования на инциденты безопасности и восстановления после них.

Сотрудничество с правоохранительными органами – взаимодействие с государственными структурами для предотвращения и расследования киберпреступлений.

Инвестиции в технологии безопасности – внедрение современных технологических решений для защиты от киберугроз.

Эти мероприятия помогают создать надежную основу для защиты информационных активов, что способствует устойчивому развитию регионов и обеспечивает их экономическую и социальную стабильность [3].

Для укрепления информационной безопасности и способствования устойчивому развитию российских регионов можно рекомендовать следующие мероприятия:

Усиление законодательной базы – принятие и обновление законов, регулирующих информационную безопасность, для обеспечения соответствия современным угрозам и вызовам.

Развитие инфраструктуры – строительство и модернизация инфраструктуры для обеспечения высокого уровня защиты данных и систем.

Образование и подготовка специалистов – создание образовательных программ и курсов для подготовки квалифицированных специалистов в области информационной безопасности.

Исследования и разработки – финансирование научных исследований и разработок в области защиты информации и кибербезопасности.

Международное сотрудничество – развитие партнёрства с другими странами и международными организациями для обмена опытом и лучшими практиками.

Создание центров реагирования на инциденты – организация специализированных центров, которые будут координировать действия в случае кибератак.

Повышение кибергигиены – пропаганда основ кибергигиены среди населения для повышения уровня личной информационной безопасности.

Эти мероприятия помогут создать многоуровневую систему защиты, которая будет способствовать безопасности, стабильности и процветанию российских регионов.

Таким образом, информационная безопасность является неотъемлемой частью стратегии устойчивого развития, поскольку она способствует созданию надёжной и безопасной среды для прогресса регионов. В эпоху трансформации, которая характеризуется быстрым развитием технологий и глобализацией, информационная безопасность играет критически важную роль, так как является фундаментом для устойчивого развития и прогресса в современном мире.

Список литературы

1. Бойченко О.В. Формирование политики информационной безопасности страны и ее регионов / О.В. Бойченко, Д.В. Иванютина // Экономика строительства и природопользования. – 2021. – №1 (78). – С. 53–60. DOI 10.37279/2519-4453-2021-1-53-60. EDN JRFAIL

2. Кушнир С.И. Некоторые проблемы информационной безопасности и последствия их игнорирования / С.И. Кушнир, М.С. Кушнир // Актуальные вопросы современной науки и образования: материалы XI науч.-практ. конф. с междунар. участ. (Мурманск, 4 март 2024 г.) / редкол.: И.В. Богданов [и др.]. – Чебоксары: Среда, 2024. – С. 81–83. EDN WTGTTI

3. Догучаева С.М. Анализ современных проблем информационной безопасности в российских компаниях / С.М. Догучаева // Риск: ресурсы, информация, снабжение, конкуренция. – 2022. – №2. – С. 65–68. EDN JXIBRK