ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ

Еникеев Ильхам

студент 2 курса, направление «Экономика», Филиал Казанского (Приволжского) федерального университета г. Джизаке, Узбекистан

A B S T R A C T

В статье рассматриваются основные аспекты обеспечения информационной безопасности в условиях цифровизации, включая защиту персональных данных, противодействие киберугрозам, обеспечение безопасности инфраструктуры, а также правовые и организационные меры по минимизации рисков. Особое внимание уделяется необходимости разработки комплексных стратегий управления киберрисками, укрепления международного сотрудничества и повышения уровня цифровой грамотности, как среди населения, так и среди организаций

A R T I C L E I N F O

Article history:
Received 19 Mar 2024
Received in revised form 24 Apr 2024
Accepted 27 May 2024

Keywords:
информационная безопасность, киберугроз, киберриск, цифровая экономика, персональные данные, комплексная стратегия, экономическая информация.

INTRODUCTION

Введение.

XXI век ознаменовался стремительным развитием цифровых технологий, которые проникают во все сферы жизни общества, преобразуя экономические, социальные и политические модели. Цифровая трансформация, порождающая новую экономическую реальность, известную как «цифровая экономика», несет в себе как огромный потенциал для прогресса, так и серьезные риски. Одним из ключевых вызовов, стоящих перед государствами, бизнесом и отдельными пользователями в цифровой экономике, является **обеспечение информационной безопасности**.

Информационная безопасность в экономической сфере обладает определенной спецификой, обусловленной цифровизацией процессов и высокой зависимостью экономики от

автоматизированных систем. В зоне наибольшего риска находятся следующие элементы:

- ✓ **Кредитно-финансовая система** - финансовые учреждения и платёжные системы подвержены кибератакам, утечкам данных и мошенническим операциям, что может дестабилизировать экономическую стабильность страны.
- ✓ **Система государственной статистики** - компрометация данных государственной статистики способна исказить экономические прогнозы и привести к принятию неверных управленческих решений.
- ✓ **Системы бухгалтерского учета организаций и предприятий** - вне зависимости от формы собственности, уязвимость бухгалтерских систем может привести к финансовым потерям, а также искажению налоговой и финансовой отчетности.
- ✓ **Учетные и информационные автоматизированные системы федеральных органов исполнительной власти** - нарушение работы данных систем ставит под угрозу управление государственными процессами и эффективное функционирование ведомств.
- ✓ **Системы сбора, обработки, хранения и передачи экономической информации** - налоговая, финансовая, таможенная информация, а также данные о внешнеэкономической деятельности являются критическими для поддержания национальной экономической безопасности. Любое нарушение их целостности может негативно сказаться на экономике в целом.

Эффективное обеспечение информационной безопасности в этих сферах требует внедрения современных защитных технологий, регулярного мониторинга угроз и принятия, стратегических мер по минимизации рисков.

Основная часть.

Современная цифровая экономика сталкивается с рядом серьезных угроз, связанных с защитой информации. Эти угрозы не всегда очевидны, но все они реальны и могут нанести значительный ущерб экономическим процессам. Основные угрозы информационной безопасности в цифровой экономике включают:

- **Киберпреступления** - взломы информационных систем, особенно банковских и финансовых учреждений, могут привести к краже финансовых средств, данных клиентов и дестабилизации работы всей системы.
- **Технологическая зависимость** - Россия остается в значительной степени зависимой от зарубежных технологий и средств защиты информации. Это создает риски для национальной безопасности, поскольку использование иностранных решений может привести к уязвимости перед внешними угрозами.
- **Деятельность коммерческих структур** - на внутреннем рынке присутствуют как отечественные, так и зарубежные компании, которые создают, защищают и обрабатывают экономическую информацию. Недостаточный контроль над их деятельностью может привести к несанкционированному доступу к конфиденциальной информации, утечкам и возможным кибератакам.
- **Хищение и искажение информации** - коммерческая тайна, которая является критической для компаний, может быть похищена или искажена. Незаконное копирование данных и нарушения в обработке информации, будь то случайные или преднамеренные, также представляют серьезную угрозу для экономики.

Для обеспечения безопасности в цифровой экономике необходимы надежные меры защиты, направленные на предотвращение и нейтрализацию как случайных, так и преднамеренных угроз информационной безопасности. Это требует постоянного совершенствования технологий защиты, а также усиления контроля за всеми участниками информационного обмена.

Для обеспечения информационной безопасности в условиях цифровой экономики реализуются следующие ключевые меры:

1. Разработка и внедрение национальных систем - создание защищенных платформ для электронных денег, платежей и электронной торговли, которые минимизируют риски внешнего вмешательства и защищают пользователей от киберугроз.

2. Разработка национальных средств защиты информации - сертифицированные отечественные решения для защиты данных играют важную роль в обеспечении безопасности экономической информации. Их внедрение в системы сбора, хранения, обработки и передачи

данных необходимо для снижения зависимости от иностранных технологий и усиления защиты конфиденциальных данных.

3. Улучшение подготовки персонала - повышение уровня квалификации специалистов, работающих с экономической информацией, через тщательный отбор и обучение. Это важно для минимизации человеческого фактора, который часто становится причиной утечек и нарушений безопасности.

4. Государственный контроль - усиление надзора за созданием и развитием систем сбора, обработки и передачи информации в таких критически важных секторах, как финансы, статистика, биржи, таможня и налогообложение. Это необходимо для предотвращения несанкционированного доступа и утечек данных.

5. Реформа системы государственной отчетности - необходимо перестроить систему так, чтобы обеспечить точность, полноту и защищенность данных, используемых государственными и частными структурами.

6. Совершенствование нормативной базы - улучшение законодательных актов, регулирующих информационные отношения в экономике, направлено на создание условий для эффективной защиты данных и регулирования информационной безопасности в стране.

Эти меры направлены на создание комплексной системы защиты данных, которая сможет эффективно противостоять современным вызовам и угрозам в сфере информационной безопасности.

В условиях цифровой экономики защита информационной безопасности (ИБ) становится важной задачей для всех сфер деятельности государства, включая внутреннюю политику. Помимо общих методов защиты, применяемых в ИБ, используются и частные, адаптированные к специфике внутренней политики. Однако некоторые угрозы и методы защиты являются универсальными и применимы к разным сферам, включая экономику, оборону и общественные институты.

Общие угрозы для внутренней политики.

1. Кибератаки и шпионаж - попытки взлома государственных систем, направленные на получение конфиденциальной информации или нарушение стабильности работы ключевых государственных структур.

2. Манипуляции в информационном пространстве - распространение фальшивой информации и дезинформации с целью подрыва доверия к государственным институтам и дестабилизации общественно-политической ситуации.

3. Незаконный доступ к государственной информации - утечка данных, содержащих важные сведения о внутренней политике, может привести к серьезным последствиям для безопасности страны.

4. Атаки на системы управления - информационные системы, используемые для контроля и управления внутренними процессами государства, становятся целью атак с целью дестабилизации политической системы.

Основные методы обеспечения информационной безопасности:

1. Защищенные коммуникационные системы - внедрение национальных систем шифрования и защищенных каналов связи для передачи данных внутри государственных органов.

2. Разработка отечественных решений в сфере кибербезопасности -создание собственных программных и аппаратных средств для защиты данных от внешних угроз, что минимизирует риски зависимости от иностранных технологий.

3. Мониторинг и контроль информационных потоков - постоянное наблюдение за информационным пространством с целью своевременного выявления дезинформации, пропаганды и других манипуляций.

4. Совершенствование нормативной базы - усиление законодательства, регулирующего информационную безопасность, включая контроль над распространением информации и обеспечение ответственности за ее утечку или манипуляцию.

Эти меры, направленные на защиту внутренней политики, имеют ключевое значение для сохранения стабильности государства и защиты его интересов в условиях глобальной цифровизации и роста числа киберугроз.

Выводы.

Информационная безопасность в цифровой экономике представляет собой ключевой аспект, обеспечивающий стабильное функционирование экономических систем и защиту интересов государства и граждан. С учетом стремительного развития технологий и увеличения числа киберугроз, необходимо принимать комплексные меры для минимизации рисков. Это включает разработку и внедрение защищенных систем обработки и передачи данных, усиление контроля над информационными потоками, а также подготовку квалифицированных специалистов в области кибербезопасности.

Система информационной безопасности должна быть адаптивной и готовой к изменениям в технологическом ландшафте, чтобы эффективно противостоять новым угрозам. Устойчивое развитие цифровой экономики невозможно без обеспечения надежной защиты данных, что, в свою очередь, способствует укреплению доверия между государством, бизнесом и гражданами. Только через совместные усилия и внедрение инновационных решений можно создать безопасную информационную среду, способствующую экономическому росту и социальной стабильности.

Список использованной литературы

1. Информационная безопасность цифровой экономики России. https://www.tadviser.ru/index.php
2. Кузнецов И.И. Информационная безопасность в цифровую эпоху: вызовы и решения // Журнал информационной безопасности. 2020. Т. 14, № 3. С. 15–22.
3. Петрова А.С., Сидоренко В.Г. Киберугрозы и их влияние на экономическую безопасность России // Экономика и управление. 2021. № 5. С. 38–45.
4. Фролов Н.П. Основы кибербезопасности: защита информации в цифровой экономике. Москва: Издательство «Экономим», 2022.
5. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
6. Научно-методические рекомендации по обеспечению информационной безопасности в организациях // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, 2020.