

ПУТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ ПРИ УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

А. Х. Мямиев¹, Ш. О. Галандарова²

¹Туркменский государственный институт экономики и управления
Туркменистан, г. Ашхабад, ул. 1972 (Ататурк), 73

²Туркменский сельскохозяйственный институт
Туркменистан, Дашогузский велаят, город Дашогуз, Рухнама 94
arismount@gmail.com

Информационная среда выступает системообразующим фактором для всех сфер жизнедеятельности общества. Она определяет состояние экономической, оборонной, социальной, политической и других составляющих национальной безопасности и влияет на безопасность различных социальных структур и институтов.

Ключевые слова: инновации, безопасность данных, информационная безопасность, цифровизация, ИТ-инфраструктура.

WAYS TO ENSURE DATA SECURITY WHEN INFORMATION SECURITY MANAGEMENT

A. Mamiyev¹, Sh. Galandarova²

¹Turkmen State Institute of Economics and Management
Turkmenistan, Ashgabat, st. Ataturk (1972), 73

²Turkmen Agricultural Institute
Turkmenistan, Dashoguz velayat, Dashoguz city, Ruhnama 94
arismount@gmail.com

The information environment acts as a system-forming factor for all spheres of society. It determines the state of economic, defense, social, political and other components of national security and affects the security of various social structures and institutions.

Keywords: innovation, data security, information security, digitalization, IT infrastructure.

В новом тысячелетии, которое характеризуется как эра информации, глобальное распространение использования Интернета, доступность информационно-коммуникационных технологий широкому кругу пользователей создали новое измерение, основанное на информационных сетях – информационное пространство. Новыми в этом пространстве являются усилия государств, организаций, групп различных целей и структур, а также частных лиц по обеспечению своих интересов путем использования информационных сетей, информационных и коммуникационных технологий законными и незаконными способами, а также беспрецедентные возможности для современного общества. необычные возможности, созданные риски. В современных условиях такие возможности и риски, угрозы появляются не только в различных сферах государства, общества, гражданской жизни и отношений, но и в сфере обороны в различных организациях и предприятиях.

Возникает новая область общественного производства, охватывающая средства и процессы создания, распространения, обработки и использования (потребления) информации. Как известно, оно стало глобальным неиссякаемым источником человечества, вступившего в эпоху развития новой, современной информационной цивилизации. Поэтому проблема обеспечения безопасности этой информации является одной из основных и важных проблем современных информационных систем.

Сегодня информационная среда активно используется во всех сферах жизни общества. С одной стороны, оно определяет состояние экономической, оборонной, социальной, политической и национальной составляющих безопасности, влияет на безопасность различных социальных структур. С другой стороны, информационная безопасность выступает как самостоятельная часть, значение и символ безопасности. Сегодня глобальные условия, характерные для социально-экономического развития цивилизации, выдвигают на первый план необходимость обеспечения информационной безопасности. Достижения в экономических и технологических отношениях привели развитые страны к вступлению в стадию постиндустриального общества, а также к обмену информацией во всех сферах жизни и работы людей.

Теория информационной безопасности постоянно развивается, поскольку в связи с развитием технологий обработки и передачи информации постоянно возникают новые проблемы обеспечения информационной безопасности.

Следует отметить, что информационная безопасность сегодня является одной из наиболее развивающихся естественных наук. Постоянно появляются новые перспективные направления исследований, а существующие открывают более глубокие научные исследования. Сегодня информация является не только уникальным и ценным товаром, но и ключевым стратегическим ресурсом. Инфраструктура государств состоит из местных и региональных телекоммуникационных и компьютерных сетей, распределенных баз данных и знаний. Возникает новый сектор общественного производства. Этот сектор охватывает средства и процессы создания, распространения, обработки и использования (потребления) информации. Кроме того, информационные технологии и ресурсы широко интегрированы во все сферы жизнедеятельности общества. В процессе информатизации изменяются методы производства, мировоззрение людей, их собственный стиль и характер жизни и т.д. происходят радикальные изменения. Во многих странах в потреблении информации участвует почти 100% населения. Это говорит о том, что информация является продуктом массового производства и массового потребления.

Чтобы защитить данные и обеспечить их безопасность, необходимо своевременное приобретение современных средств и методов защиты и их успешное внедрение. Инфраструктура информационной безопасности – интегрированный комплекс, обеспечивающий информационную безопасность ИТ-инфраструктуры государственных и коммерческих организаций.

Повышение информационной безопасности организаций можно обеспечить путем проведения многоуровневого анализа возникающих угроз.

Этап 1. Инициализация транзакции. На этом этапе на основе анализа информационных угроз определяется необходимость пересмотра принятых в организации методов защиты информации. Как правило, выявляется частичное выполнение мер защиты данных, а также требуется разработка внутренних стандартов организации для оптимальной защиты данных.

Этап 2. Управление процессом. Процесс обеспечения информационной безопасности разделен на различные отдельные процессы, и ответственность за каждый из них разделена.

Этап 3. Внедрение и мониторинг. Процесс обеспечения информационной безопасности интегрирован в бизнес-модель, согласовывается со стратегией развития организации, контролируется выполнение принятых мер, оценивается эффективность инноваций.

Этап 4. Оценивать. Необходимость корректировки принимаемых мер по обеспечению информационной безопасности определяется появлением в последнее время новых цифровых технологий с целью более полного покрытия возможных угроз.

Этап 5. Оптимизация. Осуществляется постоянное совершенствование системы информационной безопасности. Защита данных становится полностью автоматизированным явлением, интегрированным во все аспекты деятельности организации. В условиях формирования цифровой экономики вопросы информационной безопасности актуальны на государственном уровне.

На государственном уровне сформирована группа экспертов, которые на основе межведомственного сотрудничества разрабатывают политику информационной безопасности. В результате работы разрабатывается стратегия (цель) информационной безопасности. У него должны быть четкие цели, задачи и план действий для его эффективной реализации. Разработанная стратегия учитывает различные аспекты различных отраслей экономики. Национальная стратегия также включает положение, которое оценивает риски в сфере информационной безопасности. Это связано с тем, что риски возникают в разных средах с целью оптимального реагирования на них. Кроме того, важнейшим элементом стратегии является информационная инфраструктура. От этого зависит национальная безопасность государства.

На следующем этапе совершенствуется нормативно-правовое обеспечение информационной безопасности, а также разрабатываются новые правовые нормы по различным видам противоправной деятельности. Этот этап обеспечения информационной безопасности должен представлять собой непрерывный процесс обновления нормативной базы, поскольку каждый день возникают новые угрозы хранению данных, которые ранее не встречались или не получили широкого распространения.

В результате принятой стратегии и обновленной нормативной базы в сфере информационной безопасности ведется работа по утверждению отраслевых стандартов ее обеспечения. Также необходимо наладить правильный сбор информации о ситуациях, нарушающих сохранение данных. Кроме того, образовательная политика связана с обеспечением информационной безопасности, а объем собираемых и постоянно анализируемых данных в современных условиях развития цифровых технологий увеличивается. Это создает новые угрозы, борьба с которыми требует специальных профессиональных навыков. Поэтому развитие профессионального потенциала государства является важным элементом поддержки информационной безопасности на всех уровнях экономики.

Таким образом, цифровая трансформация во многих отраслях экономики привела к изменению сферы деятельности хозяйствующих субъектов, и были созданы новые риски и угрозы, ранее не существовавшие в мире. Формирование цифровой экономики во многом зависит от обеспечения информационной безопасности, а возникновение угрозы целостности цифровой информации является одним из основных направлений обеспечения безопасности как на государственном уровне, так и на уровне отдельных организаций и населения. Сегодня атаки на системы защиты данных стали более сложными и частыми. Поэтому обеспечение информационной безопасности является ведущим вопросом поддержания стабильности экономики.

Список использованных источников

1. Запечников, С. В. Информационная безопасность открытых систем: учебник для вузов / С. В. Запечников [и др.] – М. : Горячая линия – Телеком – Ч. 1 – 2006. – 686 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах: учебн. пособие для вузов / А. А. Малюк, С. В. Пазизин, Н. С. Погожий. – М. : Горячая линия – Телеком, 2004. – 147 с.
3. Будников, С. А. Информационная безопасность автоматизированных систем: учебное пособие, / С. А. Будников, Н. В. Паршин. – 2-е изд., доп. – изд-во им. Е. А. Болховитинова, Воронеж : 2011.
4. Девянин, П. Н. Информационная безопасность предприятия: учебное пособие / П. Н. Девянин [и др.] – М., 2006. – 335 с.
5. Петраков, А. В. Основы практической защиты информации: учебное пособие / А. В. Петраков – М., 2005. – 281 с.

References

1. Zapechnikov, C. B. Informacionnaya bezopasnost' otkrytyh sistem: uchebnik dlya vuzov / S. V. Zapechnikov [i dr.] – M. : Goryachaya liniya – Telekom – CH. 1 – 2006. – 686 s.
2. Malyuk, A. A. Vvedenie v zashchitu informacii v avtomatizirovannyh sistemah: uchebn. posobie dlya vuzov / A. A. Malyuk, S. V. Pazizin, N. S. Pogozhij. – M. : Goryachaya liniya – Telekom, 2004. – 147 c.
3. Budnikov, C. A. Informacionnaya bezopasnost' avtomatizirovannyh sistem: uchebnoe posobie, / S. A. Budnikov, N. V. Parshin. – 2-e izd., dop. – izd-vo im. E. A. Bolhovitinova, Voronezh : 2011.
4. Devyanin, P. H. Informacionnaya bezopasnost' predpriyatiya: uchebnoe posobie / P. N. Devyanin [i dr.] – M., 2006. – 335 s.
5. Petrakov, A. B. Osnovy prakticheskoy zashchity informacii: uchebnoe posobie / A. V. Petrakov – M., 2005. – 281 c.

© Mamiyev A, Kalandarova Sh., 2023

УДК 338.3 (476)

АСПЕКТЫ ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКОГО МЕХАНИЗМА ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА

А. А. Голубицкая

«БИП – Университет права и социально-информационных технологий»
Республика Беларусь, г. Могилев, ул. Комсомольская, 5, 212030
alla_bip@mail.ru

В статье рассмотрена определяющая роль и значение цифровой трансформации в развитии организации, рассматриваются основные цифровые навыки сотрудников организации, а также обосновывается необходимость наращивания компетенций персонала, акцентируется внимание на приоритетных областях, в которых необходимо формирование компетенций персонала.

Ключевые слова: цифровая экономика, цифровые технологии, механизм, организация, компетенции, персонал, трансформация, управление.

ASPECTS OF THE ORGANIZATIONAL AND ECONOMIC MECHANISM OF DIGITAL BUSINESS TRANSFORMATION

A. A. Golubitskaya

"BIP – University of Law and Social and Information Technologies"
5, 212030 Komsomolskaya St., Mogilev, Republic of Belarus
alla_bip@mail.ru

The article considers the determining role and importance of digital transformation in the development of the organization, considers the main digital skills of the organization's employees, and also justifies the need to increase personnel competencies, focuses on priority areas in which the formation of personnel competencies is necessary.