Пискурева Т.А., Лапшин А.П., Махов А.Н., Сергеев М.С.

Информационная безопасность ядерного объекта в условиях цифровой экономики

Аннотация: В статье рассматриваются особенности обеспечения информационной безопасности в период реализации политики перехода к цифровой экономике с учетом специфики ядерного объекта. Обращается внимание на то, что при цифровой трансформации недостаточно иметь развитую инфраструктуру. Необходимо сформировать мобильную экосистему, в которой эффективно взаимодействуют люди и цифровые технологии, выстроить устойчивую систему информационной безопасности и культуры безопасности при использовании цифровых технологий в экономической сфере.

Ключевые слова: цифровая экономика, цифровые технологии, информационная безопасность, экосистема, человеческий фактор, культура информационной безопасности

В рамках программы цифровой экономики, принятой Правительством Российской Федерации, информационная безопасность стала одним из основных направлений для дальнейшего развития информационных технологий [1]. Цифровая экономика базируется на использовании цифровых компьютерных технологий, что позволяет качественно и количественно увеличивать возможности реализации всех бизнес-процессов. Оптимизация бизнес-процессов осуществляется посредством развитой инфраструктуры, мобильной экосистемы, в которой взаимодействуют люди и цифровые технологии, культуры использования цифровых технологий, которая подразумевает цифровые компетенции сотрудников и культуру безопасности при использовании информационных технологий. Вместе с тем, подобная цифровая трансформация сопровождается и определенными рисками: цифровая модель экономики повышает степень уязвимости информации. Рост количества нарушений информационной безопасности в условиях цифровизации экономики связан с постоянным усложнением и ростом масштабов применения цифровых технологий. В последние годы как крупные,

так и малые организации столкнулись с более частыми и более серьезными информационными атаками на бизнес. Потеря данных ведет ко многим отрицательным результатам: подрыв деловой репутации, снижение конкурентоспособности, финансовые потери в случае мошенничества, срыв производственных планов, поставок, а также рост затрат из-за необходимости восстановить утерянную информацию [2]. Воздействия на информационный ресурс предприятия могут принимать различные формы, быть случайными или преднамеренными, носить естественный или искусственный характер. Также это могут быть непрофессиональные действия сотрудников, преднамеренные действия, сбои и отказы ИТ-оборудования, нелегальное копирование и использование информации, заражение вирусами информационных систем, стихийные бедствия и аварии, шпионаж, хакерское воздействие и прочие внутренние и внешние воздействия. В связи с этим, формирование цифровой экономики неразрывно связано с обеспечением информационной безопасности [3].

В условиях цифровой экономики каждому ядерному предприятию необходимо регулярно оценивать уровень своей информационной безопасности, отвечая на следующие вопросы:

- Насколько рационально распределены финансовые ресурсы между кадровым обеспечением предприятия и цифровыми технологиями, применяемыми в экономической сфере и технологиями, направленными на защиту данных? Важно учесть, что наем нового персонала без повышения квалификации в области цифровых технологий является малоэффективным способом поддержания эффективности деятельности и обеспечения конкурентоспособности, при этом важно использовать все доступные возможности по защите данных.
- Созданы ли на предприятии условия для внедрения современных цифровых технологий в экономической сфере и в области защиты информации? Необходимо, чтобы внедрению новых технологий предшествовало планирование и создание условий их эффективного применения, что позволит снизить количество сбоев и ошибок, а, значит, сократить затраты на выстраивание процесса функционирования техники и технологии.
- Каким образом, с использованием какого ресурса оценивается важность тех или иных мероприятий по обеспечению

информационной безопасности? Своевременный анализ уровней информационной защиты данных поможет оптимально оценить вклад различных средств обеспечения информационной безопасности.

- Насколько рационально обеспечивается информационная безопасность на всей цепочке оказания услуг или выполнения работ? Предприятие взаимодействует с множеством контрагентов, с которыми оно обменивается данными, поэтому важно проанализировать безопасность передачи информации другим экономическим субъектам.
- Эффективно ли ответственные за информационную безопасность предприятия справляется с задачами по обеспечению информационной безопасности в рамках цифровой экономики? Управление конфигурацией ИТ-оборудования, внедрение и управление средствами защиты информации, наличие цифровых компетенций у сотрудников является важнейшим элементом формирования информационной защиты. Повышение информационной безопасности ядерного предприятия может быть обеспечено через проведение многоступенчатого анализа возникающих угроз.

Выявление и анализ угроз. На данном этапе проводится выявление и анализ угроз, которые возникают при внедрении новых информационных технологий в научно-производственную и финансовую деятельность предприятия.

Разработка мероприятий по усовершенствованию способов и методов защиты информации. На основе анализа возникающих информационных угроз определяется потребность в пересмотре способов обеспечения сохранности данных. Необходимо, чтобы итогом этой работы стала стратегия информационной безопасности с ясными целями, задачами и планом мероприятий. Стратегия должна включать механизмы оценки рисков в области информационной безопасности. Отдельным элементом стратегии должна стать критически важная информационная инфраструктура предприятия, описание способов её оценки, классификации, защиты в рамках внедрения системы ГосСопка.

Реализация мероприятий и контроль. Процесс обеспечения информационной безопасности интегрируется в бизнес-модель, согласуется со стратегией развития предприятия, проводится

контроль за выполнением принятых мероприятий, оценивается результативность нововведений. Применяется управление по бизнес – процессами, при котором обеспечение информационной безопасности разделяется на отдельные процессы, распределяется ответственность за каждый из них.

Прогнозирование и внедрение. Дальнейшее внедрение цифровых технологий с целью усовершенствования финансово-экономической деятельности предприятия и при этом обеспечение полного охвата возможных угроз.

Развитие и оптимизация. Осуществляется непрерывное совершенствование системы обеспечения информационной безопасности: защита данных становится полностью автоматизированным процессом, интегрированным во все направления деятельности предприятия.

Необходимо отметить, что с переходом к цифровой экономике обеспечение информационной безопасности неразрывно связано с обучением и подготовкой кадров. В современных условиях развития цифровых технологий в экономической сфере создает новые угрозы, для борьбы с которыми требуются специальные профессиональные знания и навыки.

Важным направлением работы в рамках развития цифровой экономики и обеспечения безопасности информации является формирование культуры информационной безопасности, которая подразумевает не только применение современных технических средств и технологий, но и грамотные, ответственные действия квалифицированного персонала, получившего необходимое профессиональное обучение, освоившего безопасные приёмы работы с техническими средствами и программным обеспечением и осознающего приоритетность и важность информационной безопасности, основанной на мотивации поступков и действий, ответственности за порученное дело [4]. Основной целью работы по культуре информационной безопасности является повышение персональной ответственности специалистов при обращении с информацией. Совершенно очевидно, что эффективность технических мер по защите информации во многом зависит от осознания особой важности проблем информационной безопасности всеми сотрудниками ядерного предприятия.

Таким образом, цифровая трансформация, проводимая во многих отраслях экономики, привела к тому, что изменился масштаб деятельности экономических субъектов и появились новые риски и угрозы, с которым раньше мир не сталкивался. Защищенность информационных ресурсов и информационных систем, применяемых в научно-производственной и финансово-экономической деятельности предприятий, имеет стратегическое значение на ядерном объекте, где финансово-экономическая деятельность выстроена по бизнес-процессам, которые реализуются посредством внедрения новых информационных технологий. Применяемые способы защиты информации, такие как, криптографические средства, электронные цифровые подписи, идентификация и аутентификация проверки подлинности, аттестация объектов информатизации по требованиям информационной безопасности, импортозамещение программного обеспечения, культура информационной безопасности должны стать непрерывным процессом, так как с каждым днем появляются угрозы сохранности данных, с которыми ранее общество не сталкивалось, либо они не проявлялись столь масштабно. Подчеркнем, что в современных условиях цифровизации затраты на обеспечение информационной безопасности и защиты информационного ресурса предприятия – не расходы, а инвестиции, направленные на увеличение доходов в будущем. Для ядерного объекта эти инвестиции уменьшают риск утечки ценной информации и её несанкционированного распространения, а также снижают ущерб и затраты на ликвидацию последствий инцидентов при различной масштабности их проявления.

Литература:

1. Программа «Цифровая экономика Российской Федерации». Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р.
2. *Пискурева Т.А.* Совершенствование управленческих систем как условие успешного функционирования организации //Евразийский международный научно-аналитический журнал «Проблемы современной экономики». – 2009. – № 2 (30). – С. 461 – 464.