УДК 332.146.2

Н. С. Бондарев
ФГБОУ ВО «Кемеровский государственный университет», Кемерово,
e-mail: 05bns09@mail.ru

Г. С. Бондарева
ФГБОУ ВО «Кузбасский государственный аграрный университет
имени В.Н. Полецкова», Кемерово, e-mail: galina0205@mail.ru

А. В. Харитонов
Кемеровский НИИ сельского хозяйства – филиал ФГБУН Сибирский федеральный
научный центр агробиотехнологий РАН, Кемерово, e-mail: Al.kharytonov@mail.ru

Д. И. Шумелев
ФГБОУ ВО «Кемеровский государственный университет», Кемерово,
e-mail: d.shumelev@i-digit.ru

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ ЦИФРОВЫХ ПРОДУКТОВ ДЛЯ ЦЕЛЕЙ РЕГИОНАЛЬНОГО УПРАВЛЕНИЯ

Ключевые слова: информационная безопасность, цифровые продукты, региональная экономика и управление, угрозы информационной безопасности.

В статье исследованы аспекты информационной безопасности при внедрении цифровых продуктов для целей регионального управления на примере Кемеровской области-Кузбасса. Описаны требования Федерального закона №187-ФЗ «О безопасности критической информационной инфраструктуры» при разработке программного обеспечения для целей регионального управления. Представлены требования основного регулятора в системе цифрового развития региона – Министерства цифрового развития и связи Кузбасса. Представлены угрозы информационной безопасности при внедрении цифровых продуктов, определены требования региональных органов власти к цифровым продуктам, представлены параметры защищенности информационных ресурсов на примере двух внедряемых web-приложений: «Система управления мониторингом состояния объектов жилищно-коммунального хозяйства (теплотрасс, благоустройства (газоны, парки, городские леса), зданий (кровля, фасады), в части модуля земельного надзора (по землям сельскохозяйственного назначения)» и «Система управления мониторингом строительных работ на объектах, прошедших государственную экспертизу», подлежащих включению в реестр информационных систем Кемеровской области-Кузбасса. Описаны используемые для среды приложений комплекс безопасности «Континент», который обеспечивает защиту информации, передаваемую по открытым каналам. Рассмотрено соответствие Требованиям о защите информации, не содержащей государственную тайну, а также защищенные сети для защиты рабочих мест от внешних и внутренних сетевых атак.

N. S. Bondarev
Kemerovo State University, Kemerovo, e-mail: 05bns09@mail.ru

G. S. Bondareva
Kuzbass State Agrarian University named after V.N. Poletskov, Kemerovo,
e-mail: galina0205@mail.ru

A. V. Kharitonov
Kemerovo Research Institute of Agriculture – branch of the Siberian Federal Research
Center for Agrobiotechnology of the Russian Academy of Sciences, Kemerovo,
e-mail: Al.kharytonov@mail.ru

D. I. Shumelev
Kemerovo State University, Kemerovo, d.shumelev@i-digit.ru

ASPECTS OF INFORMATION SECURITY IN THE IMPLEMENTATION OF DIGITAL PRODUCTS FOR REGIONAL MANAGEMENT PURPOSES

Keywords: information security, digital products, regional economy and management, threats to information security roll stand, faced strip, dynamic factor, bearing stress, elastic interaction.

The article examines the aspects of information security in the implementation of digital products for regional management purposes using the example of the Kemerovo region-Kuzbass. The requirements of Federal Law No. 187-FZ "On the Security of critical Information Infrastructure" in the development of software for regional management purposes are described. The requirements of the main regulator in the digital development system of the region – the Ministry of Digital Development and Communications of Kuzbass – are presented. The threats to information security during the introduction of digital products are presented, the requirements of regional authorities for digital products are defined, the parameters of the security of information resources are presented using the example of two web applications being implemented: "A management system for monitoring the condition of housing and communal services (heating mains, landscaping (lawns, parks, urban forests), buildings (roofs, facades), in terms of the module of land supervision (for agricultural lands)" and "Management system for monitoring construction works at facilities, which have passed the state examination", to be included in the register of information systems of the Kemerovo region-Kuzbass. The security complex "Continent" used for the application environment is described, which ensures the protection of information transmitted through open channels. Compliance with the Requirements for the protection of information that does not contain state secrets, as well as secure networks to protect workplaces from external and internal network attacks, are considered.

Введение

Современная региональная экономика и управление направлены на всестороннее использование цифровых продуктов. Это относится как к продуктам, самостоятельно разрабатываемых органами государственной власти и органами местного самоуправления, так и к тем цифровым ресурсам, которые разработаны иными участниками – хозяйствующими субъектами – для целей управления регионом. Экономическая выгода внедрения цифровых продуктов для целей регионального управления заключается в существенном сокращении оперативности принятия решения, точности и актуальности, а также в возможностях аналитики цифровой информации, использовании искусственного интеллекта.

Внедрение цифровых продуктов для целей регионального управления учитывает различные требования, включая требования региональных органов власти, реализуемых политикой информационной безопасности.

Целью исследования является исследование требований информационной безопасности при внедрении цифровых продуктов для целей регионального управления, в связи с чем, поставлены задачи выявления особенностей региональной системы информационной безопасности, состава средств защиты информационных продуктов.

Материал и методы исследования

В системе регионального управления происходят существенные сдвиги, связанные с применением информационных технологий и информационных ресурсов [1, 2]. Они направлены как внутренние процессы государственных органов власти региона, так и на внешние элементы управления [3]. Данные процессы нуждаются в государственном регулировании, так как затрагивают уже не только коммерческий сектор. Разработка, внедрение, эксплуатация цифровых продуктов требует использование аналитических методов, позволяющих определить соответствие установленным критериям безопасности, технико-технологическим характеристикам, ресурсным компонентам операционной среды [4, 5].

Материалы для исследования определяются исходя из требований регионального управления для целей исполнения своих регуляторных функций, а именно разрабатываемые и внедряемые цифровые продукты как собственно государственные, так и разработанные частным сектором [6]. Применяемые для регионального управления цифровые продукты должны быть построены на информационных технологиях, программных средствах, обеспечивающих качественное исполнение государственных услуг. В связи с чем исследуются особые требования предъявляются к системе безопасности, особенно для информации ограниченного доступа, где кроме стандартного перечня параметров защищенности должны соблюдаться дополнительные параметры идентификации категории пользователей, электронные цифровые средства, такие как цифровая подпись [7].

Так как параметры защиты информации используются в связи с тем, что внутренняя среда реализации цифровых продуктов подвержена угрозам – модифицированию, копированию, уничтожению, к материалам исследования относится выявление угроз информационной безопасности, для устранения которых изучается система на предмет своевременности, эффективности и оперативности.

Результаты исследования и их обсуждение

Внедрение цифровых продуктов учитывает необходимые требования информационной безопасности Кемеровской области – Кузбасса. Цифровые продукты, используемые на территории региона, учитывающие местные требования и условия эксплуатации, формируют региональный рынок цифровых продуктов, который динамично развивается. Основой развития регионального рынка цифровых продуктов является наличие информационно-коммуникационной цифровой среды. Так по данным региональных органов статистики на 2023 год более 26% организаций области используют «облачные» сервисы, порядка 5% – технологии искусственного интеллекта, 12,2% – технологии Интернета вещей, порядка 18% – цифровые платформы и в целом более 50% организаций имеют веб-сайты в сети Интернет [8]. Население также взаимодействует с органами государственной власти и местного самоуправления, используя цифровые ресурсы – более 80% – Интернет (веб-сайты и порталы госуслуг, мобильные приложения, электронную почту, терминалы самообслуживания) [8]. Для того, чтобы функционировать на региональном рынке цифровых продуктов, все эти ресурсы должны соответствовать определенным требованиям.

В основе данных требований является создание в регионе устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех пользователей, которая нейтрализует простой информационных систем в результате компьютерных атак [9]. Так 19 % населения региона за 2023 год сталкивались с проблемами при получении госуслуг, в том числе 15% – из-за технических сбоев [8].

При разработке средств защиты предлагается преимущественное использование отечественного программного обеспечения, прежде всего государственными органами, органами местного самоуправления, обеспечивающего информационную безопасность региональных объектов критической информационной инфраструктуры в соответствии требований Федерального закона №187-ФЗ «О безопасности критической информационной инфраструктуры».

Региональные цифровые продукты учитывают требования, предъявляемые основным регулятором в системе цифрового развития Кемеровской области, которым выступает Министерство цифрового развития и связи Кузбасса, производящее анализ текущей ситуации, определяющее потребности региона в использования компьютерного, серверного и телекоммуникационного оборудования, программного обеспечения российского производства в органах государственной власти Кемеровской области – Кузбассе [10].

Цифровые продукты – интегрируемые web-приложения для целей управления регионом «Система управления мониторингом состояния объектов жилищно-коммунального хозяйства (теплотрасс, благоустройства (газоны, парки, городские леса), зданий (кровля, фасады), в части модуля земельного надзора (по землям сельскохозяйственного назначения)» и «Система управления мониторингом строительных работ на объектах, прошедших государственную экспертизу» Кемеровского государственного университета подлежат включению в реестр информационных систем Кемеровской области-Кузбасса. В данном реестре на 2024 год числится 32 информационных системы, которые являются ядром регионального рынка цифровых продуктов в системе управления областью.

Кемеровский государственный университет как разработчик цифровых продуктов, интегрируемых web-приложений, заключает соглашение об информационном взаимодействии с Министерством цифрового развития и связи Кузбасса. На основании заключенного соглашения появляется возможность подать заявку на включение информационной системы в реестр информационных систем Кемеровской области-Кузбасса, которое далее анализируется специалистами информационной безопасности управления информационной безопасности и связи Министерства цифрового развития и связи Кузбасса.

Учет данных требований увеличивает эксплуатационную стоимость цифровых продуктов, отметим, что затраты организаций на внедрение и использование цифровых технологий в 2022 году по сравнению с 2020 годом возросли почти в два раза – с 8953,8 млн руб. до 15151,7 млн руб., а на оплату услуг сторонних организаций и специалистов, связанных с внедрением и использованием цифровых технологий – более чем в 2 раза – с 1,5 млрд. руб., до 4,2 млрд.руб. [8]. К тому же в дополнении

к соглашению об информационном взаимодействии заключается соглашение об установлении межсетевого взаимодействия на базе ресурсов «Континен», помимо заявки на подключение к инфраструктуре ЦОД и заявки на технический доступ к ресурсу, что также увеличивает стоимость цифровых продуктов. Комплекс безопасности «Континент» является межсетевым экраном. В режиме межсетевого экрана осуществляется расширенный контроль протоколов и приложений; защита от вредоносных веб-сайтов, URL-фильтрация по категориям, антивирус и модуль GeoProtection. Используемые для среды приложений комплекс безопасности «Континент» осуществляет криптографическую защиту информации, так как часть контента между программой и конечным пользователем передается по открытым каналам и может быть перехвачена или модифицирована.

Средства безопасности позволяют определить возможные сценарии компьютерных атак, потенциальные действия нарушителей и угрозы безопасности информации, которые могут привести к компьютерным инцидентам [11]. При выборе сценария учитывается осведомленность о системах и мерах защиты объекта, возможность использования методов социальной инженерии для получения доступа к системам, способность внедрения программных закладок, использование уязвимости и создания специализированных средства для атак.

Следующая стоимостная характеристика цифровых продуктов связана с учетом требований федеральной службы по техническому и экспортному контролю – на объекте информатизации (в данном случае информационная среда разработчика – ФГБОУ ВО «Кемеровский государственный университет») должна проводиться аттестация на предмет соответствия Требованиям о защите информации, не содержащей государственную тайну. Для чего с соответствующими организациями, проводящими аттестацию, заключается договор, стоимость которого включается в состав цены на цифровой продукт.

Кроме всего прочего при разработке Web-приложения «Система управления мониторингом состояния объектов жилищно-коммунального хозяйства (теплотрасс, благоустройства (газоны, парки, городские леса), зданий (кровля, фасады), в части модуля земельного надзора (по землям сельскохозяйственного назначения)» для защиты рабочих мест от внешних и внутренних сетевых атак используется подключение к защищенным сетям. Защита доступа к ресурсам осуществляется по зашифрованному каналу связи, способному создавать и управлять ключевой информацией; шифровать файлы и данные в оперативной памяти; шифровать IP-трафик; вычислять значение хеш-функции; защищать TLS-соединения; реализовывать назначение электронной подписи.

Все эти факторы составляют особенности функционирования регионального рынка цифровых продуктов.

Заключение

Таким образом, при внедрении цифровых продуктов, использующихся в целях и в системе регионального управления web-приложения Кемеровского государственного университета «Система управления мониторингом состояния объектов жилищно-коммунального хозяйства (теплотрасс, благоустройства (газоны, парки, городские леса), зданий (кровля, фасады), в части модуля земельного надзора (по землям сельскохозяйственного назначения)» и «Система управления мониторингом строительных работ на объектах, прошедших государственную экспертизу» проходят различные этапы процесса реализации системы информационной безопасности цифровых ресурсов, позволяющие минимизировать внутренние и внешние угрозы.

Безопасность информационных ресурсов, включаемых в реестр информационных систем Кемеровской области-Кузбасса, обеспечивается с помощью защиты от вредоносных веб-сайтов, URL-фильтрации по категориям, антивирусными программами, криптографической защитой информации, наличием защиты от проникновения со стороны сетей общего пользования, защитой рабочих мест от внешних и внутренних сетевых атак.

Всё это с одной стороны обеспечивает безопасность информационных ресурсов, используемых в целях регионального управления, с другой – увеличивает временной лаг внедрения продуктов и увеличивает экономические затраты на величину средств, используемых на представленных стадиях. Данные параметры обязательно необходимо учитывать при проектировании и внедрении информационных ресурсов в целях регионального управления, для обеспечения баланса интересов разработчика, органов государственного управления и пользователями.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках соглашения о предоставлении из федерального бюджета грантов в форме субсидий от 30 сентября 2022 г № 075-15-2022-1195.

Библиографический список

1. Назаров Д.М., Назаров А.Д. Анализ семантики понятий экономическая безопасность и информационная безопасность в цифровой экономике // Международный журнал прикладных наук и технологий Integral. 2023. № 4. С. 1239-1248.

2. Хетагурова Т.Г., Хетагурова И.Ю., Соскиева З.В., Багиева М.Г. Информационная безопасность в цифровой экономике // Экономика и управление: проблемы, решения. 2023. Т. 5, № 1(133). С. 128-132. DOI: 10.36871/ek.up.p.r.2023.01.05.016.

3. Бондарев Н.С. Развитие земельного контроля в угольных регионах (на примере Кемеровской области – Кузбасса) // Уголь. 2023. № 8(1170). С. 79-83. DOI: 10.18796/0041-5790-2023-8-79-83.

4. Стоякина Е.Н., Калинина Г.В. Информационная безопасность в цифровых реалиях // Инновационная экономика: перспективы развития и совершенствования. 2023. № 3(69). С. 146-151.

5. Рудакова Е.В. Информационная безопасность в сети «Интернет» // Актуальные проблемы социально-гуманитарного и научно-технического знания. 2024. № 1(37). С. 14-15.

6. Новикова А.В. Общественно-политический процесс и информационная безопасность Забайкалья как защищенность национальных интересов // Вестник Забайкальского государственного университета. 2022. Т. 28, № 5. С. 70-76. DOI: 10.21209/2227-9245-2022-28-5-70-76.

7. Салов И.В., Байрушин Ф.Т., Абрамов И.Р. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе // Евразийский юридический журнал. 2023. № 8(183). С. 427-428. DOI: 10.46320/2073-4506-2023-8-183-427-428.

8. Территориальный орган Федеральной службы государственной статистики по Кемеровской области – Кузбассу. URL: https://42.rosstat.gov.ru/folder/38707 (дата обращения: 15.10.2024).

9. Квинт В.Л., Алимурадов М.К., Астапов К.Л. и др. Стратегирование экономического и инвестиционного развития Кузбасса. Кемерово: Кемеровский государственный университет, 2021. 364 с. DOI: 10.21603/978-5-8353-2724-9.

10. Даниленко А.А., Шарыпова Т.Н. Информационная безопасность как необходимое условие для цифровой экономики // Инновации. Наука. Образование. 2021. № 48. С. 1341-1344.

11. Бондарев Н.С. Анализ информационных ресурсов агропромышленного комплекса Кемеровской области // Экономика и предпринимательство. 2015. № 1(54). С. 253-257.

12. Широков И.С. Информационная безопасность в рамках электронной демократии // Вестник Забайкальского государственного университета. 2021. Т. 27, № 10. С. 78-84. DOI: 10.21209/2227-9245-2021-27-10-78-84.