УДК 334.021.1

И. И. Краснова[1], **Чэнь Юйин**[2]
Институт бизнеса БГУ, Минск, Беларусь,
[1]irinakrasnova0509@gmail.com, [2]hongzhaji0621@gmail.com

ПУТИ ПОСТРОЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Эта статья посвящена изучению предыстории и подходов к построению безопасности корпоративных сетей. Процесс модернизации развития цифровой экономики требует усиления сетевой безопасности предприятий.

Ключевые слова: *информационная модель предприятия, сетевая безопасность, алгоритм шифрования данных, осведомленность о безопасности*

I. Krasnova[1], **Chen Yuying**[2]
School of Business of BSU, Minsk, Belarus,
[1]irinakrasnova0509@gmail.com, [2]hongzhaji0621@gmail.com

WAYS TO BUILD ENTERPRISE NETWORK SECURITY IN THE DIGITAL ECONOMY

This article is devoted to studying the background and approaches to building security for corporate networks. The process of modernizing the development of the digital economy requires strengthening the network security of enterprises.

Keywords: *enterprise, information construction, network security, data encryption algorithm, security awareness*

Работа и развитие предприятий неотделимы от процессов информатизации. Построение качественной информационной модели способствует повышению качества продукции предприятия. В то же время вопросы сетевой информационной безопасности всегда были важным фактором, ограничивающим строительство модели информатизации. Чтобы изменить вышеуказанную ситуацию, предприятиям необходимо искать решения, закладывая основу для устойчивого развития. Рассмотрим основные направления создания эффективной модели информатизации предприятия.

1. Безопасность сетевых данных — ключевое направление технологических инноваций.

В эпоху цифровой экономики и искусственного интеллекта киберпространство стало главным полем битвы международной конкуренции. В феврале 2023 года лаборатория *Цянь Паньгу* сообщила, что хакерская организация ATW в течение длительного времени проводила кибератаки, кражу данных и пропагандистскую деятельность против Китая, включая более 70 конфиденциальных данных, таких как исходные коды и базы данных важной для Китая информации, системы с участием национальных правительственных ведомств, авиации, включающих более 100 информационных единиц и более 300 информационных систем [1].

Безопасность сетевых данных является краеугольным камнем национальной безопасности и основой всех технологических, инновационных и промышленных цепочек. В настоящее время бурно развиваются новые технологии, такие как большие данные, 5G и искус-

ственный интеллект, и появились новые сценарии, такие как «умные города», «умное правительство» и «фабрики черного света». Большие модели генеративного искусственного интеллекта, представленные *ChatGPT и Sora,* не только меняют производство и образ жизни людей, но и усиливают угрозы безопасности:

– с точки зрения сети. Интернет усугубил потери от инцидентов безопасности. Как только объекты Интернета вещей потеряют связь, произойдет авария, приводящая к потерям жизни, денег и возможностей. Например, если связь подключенных автомобилей нарушена, машина может разбиться и люди погибнут; если производственное оборудование потеряло управление, работы и производство могут быть приостановлены, также могут пострадать сервисные объекты.

– с точки зрения данных. Три основных изменения в данных привели к увеличению количества преступлений, связанных с кражей данных и вымогательством. Это следующие проблемы.

Во-первых, трудно отличить истинное и ложное поведение при манипулировании данными, и хакеры могут совершать «плохие поступки» под прикрытием законности.

Во-вторых, трудно контролировать эти нарушения. Администраторы, технические специалисты и операторы могут действовать таким образом, который ставит под угрозу безопасность данных.

В-третьих, бэкдоры трудно предотвратить, и они стали «отличным» оружием для уничтожения данных. мошенничества и вымогательства.

– с точки зрения вычислений. Услуги искусственного интеллекта и услуги вычислительных систем усугубляют риски утечек и искажения информации. Возьмем, к примеру, *ChatGPT* для помощи в офисе. Согласно статистике, 11 % контента, вставленного сотрудниками в *ChatGPT*, представляет собой конфиденциальные данные. Если возникнет проблема с данными, это скорее всего приведет к потере основной конкурентоспособности компании, кроме того, если большая модель будет умышленно искажена, будут выданы неверные результаты, что приведет к разрушительным последствиям [2].

В последние годы развитые страны Запада представили соответствующие стратегические планы по продвижению новых технологий сетевой безопасности, таких как «нулевое доверие» [3] и технология 5G, посредством законодательного регулирования. Продолжается увеличение инвестиций в создание приложений для технологических исследований и разработок. Сетевая безопасность стала своего рода «жесткой силой». Тот, кто возглавляет технологические инновации, может занять командные высоты в киберпространстве. Компании, занимающиеся сетевой безопасностью, должны продолжать внедрять технологические инновации.

2. Подходы к управлению сетевой информационной безопасностью при построении информационной модели предприятия.

Это могут быть следующие мероприятия:

– Усиление системы безопасности.

В целях дальнейшего повышения научности и безопасности управления сетевой информационной безопасностью при построении информатизации предприятия особенно важно активно создавать полную систему управления сетевой безопасностью и надзором. Это даст возможность в наибольшей степени избежать риска воздействия сетевых вирусов на этапе практического применения после завершения построения модели информатизации. Чтобы обеспечить эффективность приложений компьютерной информатизации с точки зрения защиты от вторжения сетевых хакеров, предприятиям необходимо использовать информационные технологии для проведения комплексных проверок компьютеров, использовать антивирусное программное обеспечение, создание межсетевых экранов и другие методы для

постоянного улучшения компьютерной безопасности. Разработка систем управления сетевой безопасностью и надзором. Для оптимизации и работы по улучшению строго запрещено использовать незнакомые сети для подключения компьютерного программного и аппаратного оборудования для дальнейшего обеспечения безопасности и надежности. В то же время предприятия должны сочетать оптимизированные компьютерные прикладные системы с сетевыми информационными технологиями для создания систем контроля и безопасности, соответствующих реальным условиям эксплуатации, которые постепенно улучшат возможности предотвращения рисков в процессе построения корпоративной информации.

Улучшение алгоритмов шифрования данных.

Традиционные алгоритмы шифрования данных делятся на симметричное и асимметричное. Алгоритмы сетевой информационной безопасности большинства предприятий совершенствуются на основе алгоритмов симметричного и асимметричного шифрования и, наконец, образуют систему защиты передачи данных. В контексте развития новой эпохи следует уделять внимание обращению с зашифрованными данными и файловой информацией с точки зрения алгоритмов шифрования данных. Шифрование обеспечивает поддержку и помощь в обеспечении целостности и достоверности построения данных [4].

Для передачи информации данных предприятиям необходимо активно внедрять подписи и алгоритмы асимметричного шифрования, чтобы постепенно повышать уровень безопасности каналов передачи корпоративных сетей и избежать вмешательства в данные во время фактического процесса передачи. Кроме того, для достижения наилучших результатов предприятия должны подготовиться к обеспечению безопасности структур компьютерной сети, чтобы удовлетворить требования совместного построения системы защиты безопасности компьютерной сети. Необходимо внедрить инновационные алгоритмы шифрования централизованного хранения данных для серверов и компьютерных хостов для повышения уровня безопасности сети. улучшаются в течение В процессе усовершенствованных алгоритмов шифрования данных специалистов по корпоративным сетям должны своевременно находить проблемы, связанные с влиянием человеческого фактора. Для распределенных сетевых структур на основе шифрования данных требуется разумный и научно контролируемый доступ к базе данных, а также обеспечение шифрования источников и мест назначения данных.

– Развитие осведомленности о безопасности.

Чтобы повысить осведомленность соответствующего персонала предприятия о сетевой информационной безопасности, во-первых, необходимо уделить больше внимания привлечению специалистов в области сетевой информационной безопасности, совместить это с реальной ситуацией и отобрать специалистов с хорошими профессиональными качествами и профессиональными техническими знаниями. Во-вторых, следует уделить внимание подбору высококачественного персонала. Команда специалистов будет продолжать играть ведущую роль в обеспечении построения сетевой безопасности предприятий. Наконец, необходимо повысить подготовку персонала на рабочем месте, проводить регулярные исследования и обучение, чтобы сотрудники могли правильно осознавать сетевую безопасность и организовывать предприятия. Образовательные мероприятия по внутренней сетевой безопасности помогают сотрудникам предприятия строго соблюдать соответствующие нормативные требования при использовании информационных технологий в своей повседневной работе и предотвращать проблемы информационной безопасности сети предприятия. Усиление частоты проверки компьютерных систем, обеспечение регулярных обновлений, а также очистка и дезинфекция вредоносных ресурсов в программном обеспечении и системах. Кроме того, проведение работ по защите уровня сетевой безопасности зависит от типа бизнеса предприятия и сферы применения. Различия требуют различной поддержки данных, что делает

информационные каналы более качественными и обеспечивает надежность сетевой информации. Необходимо активно принимать разнообразные и комплексные меры безопасности.

Учитывая вышеизложенное, можно сделать следующие выводы. В целом, повышение уровня информационных технологий выдвинуло более высокие требования к построению сетевой информационной безопасности предприятий. Построение информационной модели предприятий не может быть отделено от поддержки облачных вычислений и других технологий. По этой причине необходимо максимально повысить уровень безопасности информатизации предприятия с точки зрения надежности и повышения осведомленности персонала о сетевой безопасности, что сыграет положительную роль в построении платформы для стабильной и непрерывной работы в безопасной среде.

Список использованных источников

1. Лаборатория Пангу. Отрубите злую руку, которая ставит под угрозу безопасность данных Китая — раскройте организацию ATW, которая без ума от кражи данных из Китая. – С. 3. [Электронный ресурс] – Режим доступа: https://www.pangulab.cn/files/The_ATW_Mystery.pdf. – Дата доступа: 22.03.2024.

2. *Глорин, С.* Конфиденциальность и защита данных в ChatGPT и других чат-ботах с искусственным интеллектом: стратегии защиты пользовательской информации, Январь 2023 г., – Международный журнал безопасности и конфиденциальности в широкомасштабных вычислениях 15 (1):1–14. DOI:10.4018/IJSPPC.325475. – С. 7. – Режим доступа: https://www.researchgate.net/publication/372304946_Privacy_and_Data_Protection_in_ChatGPT_and_Other_AI_Chatbots_Strategies_for_Securing_User_Information. – Дата доступа: 22.03.2024.

3. Архитектура нулевого доверия: что это такое и как ее достичь. – С. 3. [Электронный ресурс] – Режим доступа: https://www.al-enterprise.com/-/media/assets/internet/documents/zero-trust-architecture-ebook-en.pdf. – Дата доступа: 22.03.2024.

4. *Голиков, Т. Ю.* Обзор методов и алгоритмов шифрования данных. – С. 12. [Электронный ресурс] – Режим доступа: https://libeldoc.bsuir.by/bitstream/123456789/43720/1/Golikov_Obzor.pdf. – Дата доступа: 22.03.2024.