УДК 339.1:004.056

Информационная безопасность в сфере электронной коммерции предприятий лёгкой промышленности

Кожакина Е. О., студ.,
Любашова К. А., студ.,
Мандрик О. Г., м.э.н., ст. преп.

Витебский государственный технологический университет, г. Витебск, Республика Беларусь

Реферат. В статье представлено понятие информационной безопасности в сфере электронной коммерции предприятий легкой промышленности, рассмотрены основные проблемы и угрозы, которые связаны с обеспечением информационной безопасности, представлены методы защиты данных и предотвращения атак на электронные устройства с целью заполучения конфиденциальной информации. Сделан вывод о том, что успех в сфере информационной безопасности в электронной коммерции предприятий легкой промышленности зависит от комплексного подхода, который включает в себя множество разнообразных технологий, процессов и людей.

Ключевые слова: электронная коммерция, информационная безопасность, веб-сайт.

Актуальность работы определяется возрастающей ролью лёгкой промышленности в структуре национальной экономики Республики Беларусь и необходимостью формирования эффективных механизмов обеспечения экономической и информационной безопасности предприятий данной отрасли в условиях современных глобальных вызовов. Стремительное развитие текстильного и обувного производства в Республике Беларусь создает потребность в комплексном научном осмыслении специфики обеспечения экономической и информационной безопасности предприятий отрасли.

Научная проблема заключается в изучении и разработке основ формирования систем информационной безопасности в сфере электронной коммерции предприятий легкой промышленности в условиях развивающихся экономик, характеризующихся высокой степенью неопределенности внешней среды, ограниченными ресурсами и специфическими институциональными условиями функционирования хозяйствующих субъектов.

Объектом исследования выступают предприятия легкой промышленности Республики Беларусь как субъекты хозяйственной деятельности, функционирующие в условиях современной экономической системы.

Предметом исследования являются экономические отношения и механизмы, обеспечивающие информационную безопасность предприятий легкой промышленности в контексте специфических условий развивающейся экономики.

Целью исследования является выявление проблем и разработка рекомендаций по со-

вершенствованию системы обеспечения информационной безопасности в сфере электронной коммерции предприятий легкой промышленности в условиях развивающейся экономики Республики Беларусь.

В современном мире электронная коммерция стала неотъемлемой частью бизнеса, предоставляя компаниям и потребителям новые возможности для взаимодействия и совершения сделок. С каждым годом количество онлайн-платежей растет, и вместе с ним увеличивается объем личной и финансовой информации, обрабатываемой в сети. Однако с развитием технологий и ростом популярности электронной торговли возникают новые угрозы информационной безопасности, которые могут привести к серьезным последствиям как для компаний, так и для их клиентов.

Информационная безопасность (англ. Information Security, а также – англ. InfoSec) – теория и практика предотвращения посягательств на любую из трех составляющих безопасности информационной системы (конфиденциальность, целостность, доступность обращающейся/содержащейся в ней информации) [1].

Информационная безопасность – это защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, уничтожения или изменения.

Информационная безопасность предприятий легкой промышленности достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками. Этот процесс сопровождается оценкой эффективности плана по управлению рисками. Для того, чтобы стандартизовать эту деятельность, научное и профессиональное сообщества находятся в постоянном сотрудничестве, направленном на выработку базовой методологии, политик и индустриальных стандартов в области технических мер защиты информации, юридической ответственности, а также стандартов обучения пользователей и администраторов. Эта стандартизация в значительной мере развивается под влиянием широкого спектра законодательных и нормативных актов, которые регулируют способы доступа, обработки, хранения и передачи данных. Однако внедрение любых стандартов и методологий в организации может иметь лишь поверхностный эффект, если культура непрерывного совершенствования не привита должным образом.

Информационная безопасность в сфере электронной коммерции предприятий лёгкой промышленности – это комплекс мер, защищающих онлайн-транзакции, данные клиентов и бизнес-инфраструктуру от киберугроз, таких как мошенничество, кража данных и несанкционированный доступ.

Электронная коммерция (e-commerce) – это сфера деятельности, связанная с покупкой и продажей товаров и услуг в интернете. Термин расшифровывается как «electronic commerce», то есть «электронная коммерция» [2].

Электронная коммерция предприятий лёгкой промышленности охватывает все виды онлайн-сделок, включая покупки, продажи и денежные переводы. Это означает, что в электронную коммерцию входят все торговые и финансовые транзакции, а также биз-

нес-процессы, происходящие в интернете. Проще говоря, это все платформы, на которых сделки осуществляются в онлайн-формате.

В свою очередь, информационная безопасность в сфере электронной коммерции охватывает множество аспектов, включая защиту данных пользователей, безопасность транзакций и защиту от мошенничества. Предприятия должны принимать меры для минимизации рисков, связанных с утечкой данных, кибератаками и другими угрозами. Неправильное обращение с информацией может привести не только к финансовым потерям, но и к утрате доверия со стороны клиентов, что в свою очередь может негативно сказаться на репутации бизнеса.

Значение информационной безопасности в сфере электронной коммерции предприятий легкой промышленности становится особенно актуальным на фоне глобальных трендов, таких как увеличение числа мобильных платежей, использование облачных технологий и развитие искусственного интеллекта. Эти технологии, хотя и предлагают новые возможности для повышения эффективности бизнеса, также открывают новые векторы для атак. Киберпреступники становятся более изобретательными, используя сложные методы для обхода защитных механизмов и доступа к конфиденциальной информации.

Для успешной защиты своих активов и данных, предприятия должны не только внедрять современные технологии защиты, но и развивать культуру безопасности среди сотрудников. Обучение и повышение осведомленности о потенциальных угрозах и методах защиты являются ключевыми элементами стратегии информационной безопасности в сфере электронной коммерции не только предприятий легкой промышленности, но и их фирменных магазинов.

В настоящее время электронная коммерция имеет ряд проблем, связанных с обеспечением информационной безопасности. Выделим следующие актуальные проблемы:

1. Фишинг и социальная инженерия.

Фишинг – это метод, с помощью которого злоумышленники пытаются обманом получить конфиденциальную информацию, такую как пароли и данные кредитных карт. Социальная инженерия включает различные манипулятивные техники для доступа к личным данным пользователей. Например, злоумышленники могут рассылать фальшивые электронные письма, маскируясь под официальные сообщения банков или известных онлайн-магазинов, чтобы побудить людей раскрыть свои данные. Фишинг-атаки могут быть весьма сложными и трудноразличимыми от настоящих сообщений. Злоумышленники могут создавать поддельные веб-сайты, которые выглядят как оригиналы, чтобы обмануть пользователей и заставить их ввести свою информацию. Важно всегда проверять URL-адреса и быть осторожными при вводе конфиденциальных данных.

2. Вредоносное программное обеспечение.

Вредоносное программное обеспечение, включая вирусы, трояны и шпионские программы, может проникать на устройства пользователей через зараженные файлы или ссылки. Оно способно собирать данные, блокировать доступ к информации или даже уничтожать ее. Вредоносное программное обеспечение распространяется через электронные письма,

загрузки с ненадежных сайтов и социальные сети. Одним из самых опасных видов вредоносного программного обеспечения является программа-вымогатель (ransomware), которая шифрует данные на устройстве пользователя и требует выкуп за их расшифровку. Для защиты от таких угроз важно использовать надежное антивирусное программное обеспечение и регулярно обновлять его.

3. Атаки на веб-сайты (Web Application Firewall, WAF).

Атаки DDoS (Distributed Denial of Service attack), распределенные атаки отказа в обслуживании, направлены на перегрузку сервера, что приводит к недоступности сайта. SQL-инъекции позволяют злоумышленникам получить доступ к базе данных сайта и извлечь конфиденциальную информацию. Эти атаки могут нанести серьезный ущерб бизнесу, вызывая потерю данных, финансовые убытки и ухудшение репутации. DDoS-атаки могут быть организованы с помощью ботнетов – сетей зараженных устройств, которые злоумышленники используют для одновременной отправки множества запросов на сервер. SQL-инъекции, в свою очередь, используют уязвимости в коде веб-приложений для выполнения вредоносных SQL-запросов.

4. Угрозы внутреннего характера.

Не только внешние угрозы представляют опасность. Сотрудники предприятия, имеющие доступ к конфиденциальной информации, могут случайно или намеренно скомпрометировать данные. Внутренние угрозы могут проявляться в виде утечки данных, несанкционированного доступа или даже саботажа. Для предотвращения внутренних угроз необходимо внедрить строгие политики доступа и регулярно проводить аудиты безопасности. Обучение сотрудников основам кибербезопасности также играет важную роль в предотвращении инцидентов.

Фишинг, вредоносное программное обеспечение, атаки на веб-сайты и внутренние угрозы представляют собой серьезные риски для предприятий и пользователей. Важно не только защищать внешние данные, но и контролировать доступ к конфиденциальной информации внутри организаций. Только комплексный подход к информационной безопасности позволит сохранить доверие клиентов и защитить бизнес от финансовых и репутационных потерь.

В результате рассмотренных актуальных проблем информационной безопасности в сфере электронной коммерции предприятий легкой промышленности сформируем следующие рекомендации как методы защиты данных и предотвращения атак:

1. Обучение сотрудников основам кибербезопасности.

Это один из самых эффективных способов предотвращения атак. Исследования показывают, что большинство успешных атак начинается с человеческой ошибки. Регулярные тренинги, семинары и информирование о новых угрозах могут значительно снизить риски. Важно, чтобы все сотрудники знали, как распознавать фишинг-атаки, которые часто выглядят как легитимные электронные письма, и могли отличать их от настоящих коммуникаций.

Обучение должно охватывать не только теоретические знания, но и практические навыки. Например, создание симуляций фишинг-атак может помочь сотрудникам научиться

распознавать подозрительные сообщения и вовремя реагировать на них. Проводя такие тренинги, организации могут обнаружить слабые места в осведомленности своих сотрудников и дополнительно сосредоточиться на их обучении.

Кроме того, важно обучать сотрудников безопасному обращению с конфиденциальной информацией. Сотрудники должны понимать, какие данные являются конфиденциальными, как их защищать и какие меры предосторожности следует соблюдать при работе с электронными устройствами. Это включает в себя использование надежных паролей, шифрование данных и безопасное хранение информации.

2. Осведомленность пользователей.

Предприятия, онлайн-магазины и другие сервисы могут предоставлять своим клиентам информацию о безопасности, обучая их, как создавать надежные пароли, проверять подлинность веб-сайтов и защищать свои данные. Создание четких инструкций и рекомендаций по безопасности на веб-сайтах может помочь уменьшить риски. Например, предоставление пользователям информации о том, как устанавливать двухфакторную аутентификацию на их аккаунтах, может значительно повысить уровень безопасности.

3. Антивирусное программное обеспечение и фаерволы.

Данный метод также является важной частью стратегии защиты данных. Антивирусное программное обеспечение сканирует файлы и программы на наличие вредоносного кода, помогая предотвратить заражение систем. Фаерволы, в свою очередь, контролируют входящий и исходящий трафик, блокируя подозрительные соединения и защищая сеть от несанкционированного доступа.

Однако важно не только установить антивирусное программное обеспечение, но и регулярно обновлять его. Новые вирусы и угрозы появляются каждый день, и только обновленное программное обеспечение может эффективно защищать от них. Комплексные решения безопасности, которые объединяют антивирус, фаервол и другие инструменты защиты, могут обеспечить более высокий уровень безопасности.

4. Технологии обнаружения и предотвращения вторжений (Intrusion Detection System и Intrusion Prevention System, IDS/IPS).

Организации должны рассмотреть возможность использования технологий обнаружения и предотвращения вторжений (IDS/IPS), которые помогают выявлять и блокировать потенциальные атаки в реальном времени. Эти системы могут анализировать сетевой трафик и выявлять подозрительную активность, что позволяет быстро реагировать на угрозы.

5. Дополнительное программное обеспечение для анализа поведения системы защиты конечных устройств (Endpoint Detection and Response, EDR).

Важно также учитывать, что некоторые вредоносные программы могут быть скрытыми и не вызывать подозрений. Поэтому использование дополнительного программного обеспечения для анализа поведения, такого как системы защиты конечных устройств (EDR), может помочь в выявлении необычной активности на устройствах и предотвращении атак.

6. Регулярное обновление программного обеспечения и установка патчей.

Еще одна важная мера защиты. Многие кибератаки используют известные уязвимо-

сти в программном обеспечении. Своевременное обновление систем помогает устранить эти уязвимости и снижает риск атак. На практике это означает, что организации должны следить за выпусками обновлений от своих поставщиков программного обеспечения и немедленно их устанавливать.

7. Автоматическое обновление программного обеспечения.

Данный метод может значительно упростить этот процесс, гарантируя, что все системы всегда будут защищены от последних угроз. Однако важно также проводить регулярные проверки на наличие уязвимостей, чтобы выявлять и устранять потенциальные проблемы до того, как они смогут быть использованы злоумышленниками.

8. Специализированные инструменты для управления уязвимостями.

Для повышения уровня безопасности рекомендуется использовать специализированные инструменты для управления уязвимостями, которые могут сканировать системы и сообщать о найденных проблемах. Это позволит организациям быть проактивными в своем подходе к безопасности.

9. Аудит безопасности и тесты на проникновение.

Важно проводить аудит безопасности и тесты на проникновение, чтобы выявить слабые места в системе и улучшить общую защиту. Такие мероприятия могут включать в себя как внутренние, так и внешние оценки, которые помогают понять, насколько хорошо защищены системы от реальных угроз.

10. Многофакторная аутентификация (Multi-Factor Authentication, MFA).

Многофакторная аутентификация (MFA) добавляет дополнительный уровень безопасности, требуя от пользователей предоставить несколько форм идентификации перед доступом к учетной записи или системе. MFA может включать в себя комбинацию пароля, одноразового кода, отправленного на мобильное устройство, и биометрических данных, таких как отпечаток пальца или распознавание лица.

Использование MFA значительно усложняет злоумышленникам доступ к учетным записям, даже если они получили пароль пользователя. Это особенно важно для защиты конфиденциальной информации и финансовых данных. Внедрение MFA в организации не только улучшает безопасность, но и повышает доверие клиентов и пользователей.

Однако внедрение многофакторной аутентификации требует обучения пользователей правильному использованию этой технологии. Например, пользователи должны знать, как правильно использовать одноразовые коды и как действовать в случае подозрительной активности в своих учетных записях. Также важно предоставить пользователям возможность восстанавливать доступ к учетной записи в случае потери устройства, на которое отправляются коды.

11. Адаптивная аутентификация.

Дополнительно стоит рассмотреть возможность использования адаптивной аутентификации, которая позволяет оценивать уровень риска каждого входа в систему и требовать дополнительные факторы аутентификации только в случае необходимости. Это может улучшить пользовательский опыт, не снижая уровня безопасности.

Таким образом, в результате проведенной работы можно сделать следующие выводы:

– во-первых, в условиях стремительного роста электронной коммерции информационная безопасность предприятий легкой промышленности в этой сфере становится неотъемлемой частью эффективного функционирования бизнеса. Учитывая, что онлайн-транзакции продолжают набирать популярность, предприятия сталкиваются с новыми вызовами в области защиты данных и предотвращения кибератак. Угрозы, такие как фишинг, вредоносное программное обеспечение, атаки на веб-сайты и внутренние риски, требуют комплексного и многоуровневого подхода к обеспечению безопасности;

– во-вторых, ключевым аспектом успешной стратегии информационной безопасности является обучение и повышение осведомленности сотрудников. Без должного уровня понимания потенциальных угроз даже самые современные технологии защиты могут оказаться неэффективными. Регулярные тренинги и симуляции фишинг-атак позволяют не только обучить сотрудников, но и создать культуру безопасности внутри организации. Это создает атмосферу ответственности и бдительности, что является необходимым для минимизации рисков;

– в-третьих, использование антивирусного программного обеспечения и фаерволов – это лишь основа для защиты данных. Комплексные решения, которые включают системы обнаружения и предотвращения вторжений, а также технологии защиты конечных устройств, обеспечивают более высокий уровень безопасности. Регулярное обновление программного обеспечения и установка патчей помогают устранить уязвимости, которые могут быть использованы злоумышленниками, что также является важным элементом защиты;

– в-четвертых, не менее важным является внедрение многофакторной аутентификации, которая значительно усложняет злоумышленникам доступ к учетным записям. Это подчеркивает, что безопасность – это не только про технологии, но и про людей. Обучение пользователей правильному использованию многофакторной аутентификации и других мер безопасности – это важный шаг к защите как индивидуальных данных, так и корпоративной информации;

– в-пятых, в конечном счете, успех в сфере информационной безопасности в электронной коммерции предприятий легкой промышленности зависит от комплексного подхода, который включает в себя технологии, процессы и, что немаловажно, людей. Только таким образом предприятия смогут защитить свои активы, сохранить доверие клиентов и минимизировать финансовые потери. В условиях постоянно меняющегося киберландшафта важно не только реагировать на текущие угрозы, но и проактивно предугадывать возможные риски, создавая гибкие и адаптивные стратегии безопасности.

Список использованных источников

1. Schlienger, Thomas. Information security culture : From analysis to change : [англ.] / Thomas Schlienger, Stephanie Teufel // South African Computer Journal. – Pretoria, South Africa, 2003. – Vol. 31.

2. Мандрик, О. Г. Бизнес-модели электронной коммерции и их характеристика / О. Г. Мандрик // Экономика и маркетинг в XXI веке: проблемы, опыт, перспективы : сборник материалов XX Всероссийской научно-практической конференции, Донецк, 28–29 ноября 2024 г. / ДонНТУ. – Донецк, 2024. – С. 222–227.

УДК 331.101.262

Развитие текстильной отрасли в новых условиях: ключевые драйверы и требуемые компетенции

Стаселько В. М., м.н., асп.,
Зайцева О. В., к.э.н., доц.

Витебский государственный технологический университет, г. Витебск, Республика Беларусь

Реферат. Цель статьи – проанализировать мировые тренды трансформации текстильной промышленности и определить ключевые компетенции, необходимые для её устойчивого развития. Рассматриваются два главных драйвера изменений: экологизация и цифровизация. Описаны технологии переработки, «умные» ткани, цифровое проектирование и принципы циркулярной экономики.

Особое внимание уделено белорусской текстильной отрасли, её адаптации к новым условиям, росту экспорта, модернизации производств и развитию брендов. Также выделены вызовы, включая сырьевую зависимость и точечное внедрение эко-стандартов.

В завершение представлены четыре кластера профессиональных компетенций, необходимых для работы в условиях Индустрии 4.0 и устойчивого производства.

Ключевые слова: текстильная промышленность, мировые тенденции, профессиональные компетенции, конкурентоспособность работников.

Текстильная промышленность – одна из самых древних и важных отраслей экономики. Она играет ключевую роль в производстве одежды, мебели, технических тканей и многих других товаров, нужных в повседневной жизни. Мировая текстильная промышленность находится на переломном этапе, который можно охарактеризовать как переход от модели массового производства к модели осознанного и технологичного создания ценности. Эта трансформация затрагивает все этапы – от идеи дизайнера до утилизации вещи. Отправной точкой этого глобального сдвига стало растущее давление на отрасль со стороны двух ключевых факторов: экологии и цифровизации [2].