УДК 004.056.5:339.138

КИБЕРБЕЗОПАСНОСТЬ В МАРКЕТИНГЕ

А.Н. ЯКОВУК
(Представлено: В.А. СКОПЬЮК)

В статье автором рассмотрены меры для поддержания защищённости данных в сфере маркетинга. Изучена актуальность проблемы кибербезопасности в Республике Беларусь и составлен упорядоченный список методов надёжной защиты данных.

Внедрение информационных технологий в современном мире наблюдается повсеместно. В каждую сферу деятельности внедряется всё больше электронных информационных систем, происходит автоматизация различных процессов. А сфера Digital-маркетинга в целом использует все возможные цифровые каналы для привлечения и удержания клиентов. Это означает, что большинство процессов уже автоматизировано [1]. Несанкционированный доступ к информации, находящийся в руках маркетологов, может привести к серьёзным негативным последствиям для всего бизнеса, начиная от материального ущерба и заканчивая полной потерей доверия клиентов и угрозой потери репутации компании.

Контактная информация маркетологов обычно находится в открытом доступе, что повышает вероятность фишинговых атак. Маркетинговые инструменты, которые собирают данные или отправляют коммерческие и акционные предложения, становятся наиболее уязвимыми местами для атак. Примером таких сервисов служат WordPress, Omnisend, Monday.com [2]. В публичном доступе освещено не много примеров кибератак, направленных конкретно на сферу маркетинга, продвижения, продаж. Самая известная произошла в 2017 году, когда произошло глобальное массовое заражение вирусом «Petya». Наравне с атаками на серверы компаний всех возможных отраслей, он практически полностью остановил работу многих структур крупнейшего в мире коммуникационного холдинга WPP [1].

Тема информационной безопасности становится всё более актуальной как во всем мире, так и для Беларуси. Кибератаки сейчас являются одной из самых серьёзных угроз для бизнеса.

Обращаясь к глобальной статистике, По данным SurfShark на октябрь 2022 года, Беларусь заняла 19 место по количеству взломанных аккаунтов (за третий квартал – 539,063) [3].

Исходя из статистики, предоставляемой МВД Республики Беларусь, сумма установленного материального ущерба от совершения киберпреступлений составила в январе – октябре 2022 г. 4,1 млн. рублей, когда в 2021 году сумма составила 741,7 тыс. рублей (рисуно 1).

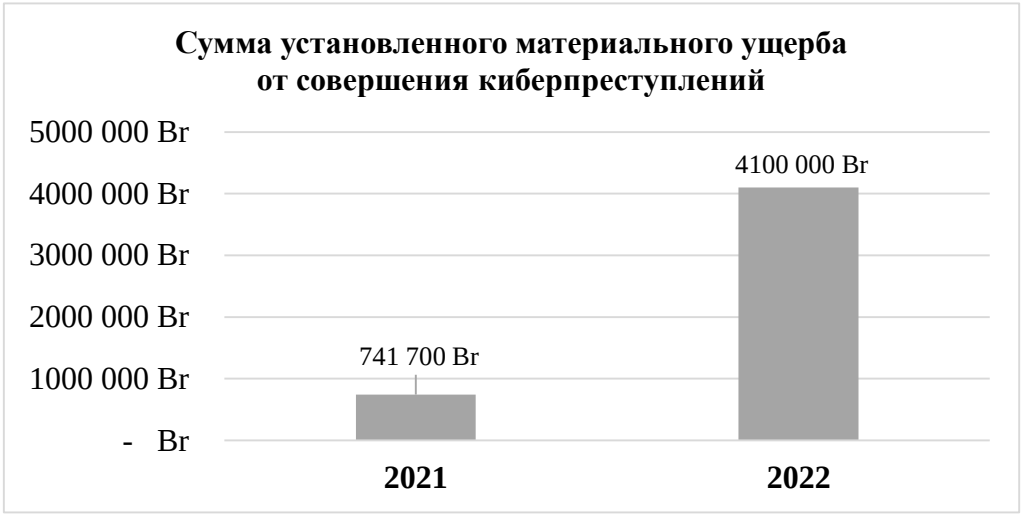

Рисунок 1. – Сумма установленного материального ущерба от совершения киберпреступлений в Республике Беларусь за 2021-2022 гг.

Источник: собственная разработка.

Под материальным ущербом понимаются финансовые потери, понесенные компанией или частным лицом в результате успешной кибератаки. Примеры материального ущерба включают кражу денег или конфиденциальных данных, повреждение программного обеспечения, убытки из-за нарушения работы системы и др.

По данным SBEL, более 50% кибератак вовсе не обнаруживается, около 70% организаций (предприятий) в мире не готовы к нарушениям безопасности, а в среднем в мире компании (организации) требуется более 6 месяцев, чтобы установить факт утечки данных [4].

Для защиты информации в Digital-маркетинге необходимо соблюдать следующие меры (таблица 1).

Таблица 1. – Меры для защиты информации в Digital-маркетинге

Мера	Описание
Контроль доступа к информации	Предусматривает разработку строгой политики безопасности, а также соблюдение следующих мер [5]: 1. Создание надёжных паролей для учётных записей работников. Безопасным паролем считается пароль, содержащий как минимум 10-12 символов, включая заглавные буквы, строчные буквы, цифры и специальные символы. Он не может быть использован в иных учетных записях работника или быть очевидным (например, "password" или "12345678"). 2. Пароли от учётных записей сотрудников должны быть надёжными и труднопод-бираемыми. 3. Пароли к корпоративным сетям должны регулярно обновляться
Надёжное шифрование данных	Процесс перевода информации в формат, который не может быть понят другими лицами, кроме тех, кто имеют права на чтение этой информации. Существует множество алгоритмов шифрования, некоторые из них - AES, RSA, DES [6]. Самым широко используемым и надёжным алгоритмом шифрования сейчас является алгоритм AES [7]. Это симметричный тип шифрования, поскольку он использует один и тот же ключ как для шифрования, так и для расшифровки данных. Он также использует алгоритм SPN, применяя несколько раундов для шифрования данных. Также не так давно стало применяться «двойное шифрование» – включены два или более независимых уровня шифрования [8]
Обучение персонала в сфере кибербезопасности	Компания должна регулярно повышать осведомлённость сотрудников в сфере кибербезопасности и маркетинговая команда должна тесно сотрудничать с IT-командами. Если прервать цепочку атак ещё на моменте проникновения в электронную систему маркетолога (например, на сайте WordPress), все возможные угрозы от взлома могут быть устранены ещё на этом этапе [9]
Использование и регулярное обновление антивирусного программного обеспечения	Для защиты от различных типов вирусов лучше всего использовать специализированные антивирусные программы и межсетевое экранирование. Объекты, которые необходимо защищать от вирусов, включают в себя рабочие станции, различные серверы (Web-приложений, файловые серверы, серверы документооборота и т.д.), интернет-шлюзы и почтовые серверы. Существуют специальные антивирусные программы («Kaspersky Security для почтовых сервисов», «Антивирус каспеского для систем хранения данных» и т.д.). Однако не все предприятия могут позволить себе подписки на специализированные антивирусные программы. В таком случае для защиты от всех видов угроз нужно использовать комплексный антивирус, самые известные из которых, «Kaspersky Security», «Dr.Web Security Space», «AVG Internet Security»
Применение резервного копирования информации	Существует множество компаний, специализирующихся на резервном копировании, обычно предоставляющие как аппаратное, так и программное обеспечение. Самыми известными на мировом рынке являются компании «Commvault» и «Veritas», на рынке Беларуси и России самой популярной является компания «RuBackup» [10]
Использование виртуальной частной сети (VPN)	Позволяет защитить данные от прослушивания и перехвата. VPN-соединение защищает от локальных попыток отслеживания и даже скрывает реальный адрес интернет-протокола с веб-сайтов и служб, к которым происходит обращение. Существуют различные технологии VPN с разной степенью шифрования. Наиболее безопасные – OpenVPN, который использует SSL/TLS. Рекомендуемыми параметрами являются шифрование AES256 с ключом RSA длиной не менее 2048 бит [11]
Регулярный аудит информационной системы	Данный тип мероприятий предназначен для проверки состояния безопасности IT-инфраструктуры, выявления возможных угроз и уязвимостей. Он может быть применен к корпоративным сетям, отдельным устройствам, сайтам, приложениям, программам, серверам и процессам. Аудиторские проверки могут проводиться как внутри компании, так и внешними экспертами [12]

Источник: собственная разработка.

По мнению автора, для повышения уровня защиты информации, нормы применения перечисленных технологий должны носить не просто рекомендательный характер, а быть обязательными для исполнения на всех предприятиях на законодательном уровне.

В Беларуси 14 февраля 2023 года был подписан Указ № 40 «О кибербезопасности». В данном документе определены нормы права, которые будут использоваться для создания и оптимизации национальной системы, обеспечивающей кибербезопасность. Благодаря комплексной системе на нескольких уровнях возможно будет предупреждать кибератаки на организации, государственные учреждения и критическую информационную инфраструктуру. Определены владельцы критических объектов информатизации, при которых в обязательном порядке будут создаваться центры кибербезопасности. В этот список вошло 27 критически важных объектов: список сюда.

Реализация указа будет осуществлена в течении 6 месяцев после публикации [13].

Создание общей национальной системы кибербезопасности – это первый шаг для Беларуси к переходу на более строгий уровень государственного контроля систем информационной безопасности. При повышении уровня государственного контроля, информация, находящаяся внутри предприятия, в том числе и в маркетинговом отделе, будет намного меньше подвержена утечкам данных.

Исходя из вышеизложенной информации, можно сделать вывод: чётко выработанная система защиты информации в сфере Digital-marketing сейчас является неотъемлемой частью всей системы информационной безопасности предприятия (организации). Сотрудникам маркетингового отдела нужно помнить о важности тех данных, с которыми они работают. Тем временем руководство предприятия должно создавать условия, при которых поддержание защищённости данных станет частью обязанностей маркетолога. Выполнение простых рекомендаций, таких как создание надёжных корпоративных паролей, установка и своевременное обновление антивирусного программного обеспечения, использование шифрования данных и VPN существенно снижает риск успешной кибератаки со стороны злоумышленников. Также обучение сотрудников маркетингового отдела и их сертификация по кибербезопасности существенно повысит шанс остановки цепочки атак на конфиденциальные данные предприятия.

ЛИТЕРАТУРА

1. Кибербезопасный маркетинг // Microsoft [Электронный ресурс]. – 2021. – Режим доступа: https://news.microsoft.com/ru-ru/features/cybersecurity-marketing-sales/. – Дата доступа: 16.02.2023.
2. Лучшие инструменты цифрового маркетинга // Begindot [Электронный ресурс]. – 2023. – Режим доступа: https://www.begindot.com/ru/. – Дата доступа: 16.02.2023.
3. Cybercrime statistics // SurfShark [Electronic resource]. – 2023. – Mode of access: https://surfshark.com/research/data-breach-impact/statistics. – Date of access: 24.02.2023.
4. Современные аспекты кибербезопасности // SBEL [Электронный ресурс]. – 2023. – Режим доступа https://security.beltelecom.by/2021/12/30/sovremennie_aspekti_kiberbezopasnosti/. – Дата доступа: 24.02.2023.
5. Советы по созданию уникальных надёжных паролей // Kaspersky [Электронный ресурс]. – 2022. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/how-to-create-a-strong-password. – Дата доступа: 24.02.2023.
6. The Best and Most Common Encryption Methods // SourceForge [Electronic resource]. – 2022. – Mode of access: https://sourceforge.net/articles/the-best-and-most-common-encryption-methods/. – Date of access: 04.03.2023.
7. What is AES encryption and how does it work // Cybernews [Electronic resource]. – 2022. – Mode of access: https://cybernews.com/resources/what-is-aes-encryption/. – Date of access: 04.03.2023.
8. Двойное шифрование // Microsoft [Электронный ресурс]. – 2023. – Режим доступа: https://learn.microsoft.com/ru-ru/azure/security/fundamentals/double-encryption. – Дата доступа: 04.03.2023.
9. Building a Cyber Security Strategy for Marketers // SecurityHQ [Electronic resource]. – 2022. – Mode of access: https://www.securityhq.com/blog/building-a-cyber-security-strategy-for-marketers/. – Date of access: 10.03.2023.
10. Стратегия резервного копирования данных // ИТЦ-М [Электронный ресурс]. – 2021. – Режим доступа: https://www.itc.by/strategiya-rezervnogo-kopirovaniya-dannyh/. – Дата доступа: 10.03.2023.
11. Использование технологии VPN для обеспечения информационной безопасности / А. Ю. Николахин. // Экономика и качество систем связи. – 2018. – №3.
12. Аудит информационной безопасности: что это, зачем и когда его проводить // Cloud.ru [Электронный ресурс]. – 2022. – Режим доступа: https://cloud.ru/ru/warp/blog/vidy-audita-informacionnoj-bezopasnosti. – Дата доступа: 15.03.2023.
13. О кибербезопасности: Указ Президента Республики Беларусь, 14 февраля 2023 г., № 40 // Президент Республики Беларусь [Электронный ресурс]. – Минск, 2023.