УДК 394:314.15
DOI: 10.25206/2542-0488-2024-9-3-149-157
EDN: NMIBGA

С. Г. СИМОНОВ
И. В. ЛЫСЕНКО

Тюменский
индустриальный университет,
г. Тюмень

РОССИЙСКИЙ БИЗНЕС В УСЛОВИЯХ РОСТА КИБЕРПРЕСТУПНОСТИ: ИЗМЕНЕНИЯ ЭКОНОМИЧЕСКОГО ПОВЕДЕНИЯ И ЗАЩИТНЫЕ МЕХАНИЗМЫ

Статья посвящена выявлению и анализу новых векторов развития киберпреступности, их локализации и предотвращения. В качестве методов исследования настоящей проблемы в работе использованы анализ вторичных данных, анкетирование, экспертная оценка. Проанализированы статистика киберпреступности в зарубежных странах и России за последние годы. Выяснено, как отечественный бизнес изменил свое отношение к безопасности информации и информационных систем компании. Представлен секторальный ландшафт киберпреступлений в РФ на 2023 год. Подробно рассмотрены новые векторы развития фишинга и определены основные ресурсы, подделываемые хакерами при проведении фишинговых атак. Особое внимание уделено фишингу по способу распространения, представляющего сегодня наибольшую опасность для российских компаний. Изучен спуфинг как новый тип кибератаки, где маскировка под легальный объект (компьютер, устройство или сеть) используется хакерами как средство проникновения в другие компьютерные сети. Дана характеристика современным видам спуфинга и тех негативных последствий для бизнеса, к которым они приводят. Указаны меры противостояния новым векторам развития киберпреступности, предпринятые на государственном уровне. Обоснован вывод, что сами по себе государственные меры поддержки и информационной защиты устраняют, скорее, последствия, а не причины высокой киберпреступности, в силу чего без участия отечественного бизнеса и населения страны проблему безопасности не решить. Отмечено консолидированное участие российского бизнеса в борьбе с киберпреступностью, нашедшее свое конкретное воплощение в создании акционерной компании F.C.C.T. Выделены ключевые направления деятельности данной компании на ИБ-рынке и результаты ее работы в 2023 году. Акцентировано внимание на том факте, что создание в стране акционерной компании F.C.C.T. далеко не в полной мере решает проблему обеспечения информационной безопасности, что, в первую очередь, касается малых и средних бизнес-структур. Заявлено, что многие из них, особенно в российских регионах, не готовы к приобретению ИБ-услуг не только финансово, но и организационно. Предложено в силу низкого запроса предпринимателей на услуги поиска уязвимостей в ПО, веб-приложениях и IT-инфраструктуре компании построение типового SOC, удовлетворяющего самым минимальным стандартам борьбы с киберпреступностью. Разработан алгоритм их достижения в виде пошагового выполнения несложных организационно-методических рекомендаций по профилактике киберпреступлений и минимизации их последствий для хозяйствующих субъектов малого и среднего форматов.

Ключевые слова: киберпреступность, фишинг, спуфинг, хакерская атака, информационная безопасность, киберугрозы и уязвимости, малый и средний бизнес.

1. Введение. Как динамично развивающаяся область кибербезопасность сталкивается с новыми вызовами ввиду появления и распространения инновационных технологий, сервисов, приложений и устройств. Развитие интернета вещей (IoT), облачных вычислений, мобильных устройств, социальных сетей, криптовалют, блокчейна, искусственного интеллекта (AI) и машинного обучения (ML)

сопровождается хакерскими атаками и киберпреступлениями. Например, IoT-устройства заражаются вредоносным ПО, которое может использоваться для создания ботнетов, проведения DDoS-атак или шпионажа. Облачные сервисы становятся скомпрометированными в случае получения мошенниками доступа к учетным данным, ключам или токенам. Мобильные устройства подвергаются фишингу, краже, потере или взлому. Социальные сети хакерами используются для распространения дезинформации, манипуляции, кибербуллинга или кражи персональных данных. Криптовалюты и блокчейн подвергаются атакам с помощью поддельных транзакций, двойных расходов, взлома кошельков или майнинга. С помощью искусственного интеллекта (AI) и машинного обучения (ML) киберпреступники создают поддельные изображения, видео, аудио или тексты, вводящие в заблуждение, обманывающие или шантажирующие корпоративных пользователей. Появление и распространение выше указанных инновационных технологий, сервисов, приложений и устройств, хотя и является одним из самых перспективных и влиятельных трендов в области борьбы с киберпреступностью, способно как повысить, так и понизить уровень безопасности информации и информационных систем компании.

2. Методы исследования. Для сбора эмпирического материала, лежащего в основе исследования проблемы борьбы с киберпреступностью, в настоящей работе использовались такие методы, как анализ вторичных данных, анкетирование, экспертная оценка.

Так, первый из них предполагал тщательное изучение материалов, которые были получены по данной тематике другими отечественными и зарубежными учеными. С помощью вторичного анализа удалось верифицировать и в известной степени интерпретировать полученные результаты исследования. Кроме того, он дал возможность заложить основы построения типового внутреннего центра мониторинга кибербезопасности (SOC — Security Operation Center), как структурного подразделения компании среднего или малого формата, которое отвечает за оперативное изучение IT-среды и реагирования на киберинциденты.

Такой метод исследования, как анкетирование, позволил выявить изменения отношения российского бизнеса к проблеме кибербезопасности, а также выяснить, какие основные корпоративные ресурсы подделывают хакеры при проведении своих атак.

Наконец, методом экспертной оценки были охвачены две группы экспертов:

— менеджеры высшего и среднего звеньев тюменских компаний, принимающих участие в федеральной программе «Производительность труда и поддержка занятости», для реализации которой Тюменская область была выбрана пилотной территорией;

— представители местных органов власти, общественных организаций и научного сообщества региона, напрямую не связанные с бизнес-деятельностью.

Благодаря применению данного метода удалось получить представление об отраслевом ландшафте запроса предпринимателей юга исследуемого региона на услуги поиска уязвимостей в ПО, веб-приложениях и IT-инфраструктуре компаний.

3. Результаты и обсуждение. Как свидетельствует международная статистика, киберпреступность

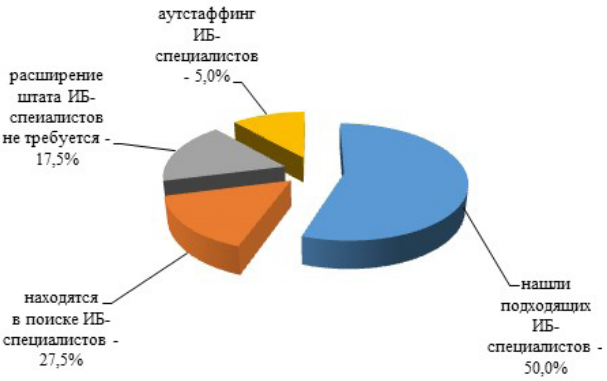

Рис. 1. Результаты ответов на вопрос «Какие изменения в штатном составе ИБ-специалистов Вы планируете на фоне возрастающих киберугроз?» [2]

Таблица 1

Секторальный ландшафт киберпреступлений в РФ на 2023 год [3]

№ п/п	Наименование наиболее привлекательных векторов кибератак на российские компании	Распределение наиболее привлекательных векторов кибератак на российские компании в порядке убывания удельных весов (в %)
1	Госсектор	37
2	Финансовая сфера	23
3	Телекоммуникационная сфера	18
4	Энергетический сектор	7
5	Нефтяная отрасль	5
6	Другие секторы, отрасли, сферы	10

во многих странах продолжает не только набирать обороты, но и менять свой ландшафт и качество. Это касается и России, оказавшейся сегодня в страновом рейтинге на восьмой позиции с показателем 5,3 % от общего количества кибератак в мире. Первые три места в этом списке заняли США (16,2 %), Индия (12,8 %) и КНР (10,4 %) [1].

Выяснилось также, что за последнее время отечественный бизнес поменял свое отношение к кибербезопасности. Это подтвердил проведенный в 2023 году компанией K2Tex опрос представителей 100 бизнес-структур из различных отраслей российской экономики (рис. 1).

Как видно из рис. 1, половина представителей опрошенных компаний уже нашла подходящих сотрудников для борьбы с киберпреступлениями, еще немногим больше четверти из них (27,5 %) пребывают в стадии поиска, а оставшиеся 5 % компаний используют аутстаффинг, одалживая ИБ-специалистов у других компаний.

Претерпел изменения и секторальный ландшафт киберпреступлений в нашей стране (табл. 1).

Добавим, что общее количество кибератак на российские компании за период 2022—2023 гг. выросло на 28 % [4]. Причем в качестве начального вектора атаки хакеры продолжают выбирать *фишинг,* который обрел новые векторы своего развития. С его помощью сегодня распространяют

шифровальщиков, инфостиллеры и другие виды вредоносного программного обеспечения (ПО), направленные на кражу ценной информации и получение доступа к IT-инфраструктуре компаний. Кстати, самым уязвимым звеном для них остаются представители малого и среднего бизнеса, не способные защититься от быстро меняющих свои схемы киберпреступников. Так, в 2023 году одной из самых популярных схем хакеров были рассылки по электронной почте, которая оказалась для них достаточно эффективной и менее затратной. Только в первом его квартале было зафиксировано свыше 800 атак шифровальщиков, когда заражение происходило через вредоносные рассылки. К концу второго квартала 2023 года общее количество фишинговых атак увеличилось в 4,6 раза, при этом каждая компания стала сталкиваться с фишингом на 24 % чаще [5].

В современной научной литературе, посвященной вопросам кибербезопасности, фишинг классифицируют по двум признакам:

а) по методу сбора данных;

б) по способу распространения.

Согласно первому признаку, выделяют:

— фейковый сайт. Хакеры используют тот же интерфейс, что у оригинала, и похожие домены, чтобы ввести пользователей в заблуждение. В адресе может быть изменен один знак. Как правило, меняют выглядящие одинаково буквы. Например, заглавная I и строчная L. Aliexpress.com и Aliexpress.com — разные домены, хотя визуально не отличаются;

— вредоносный файл. Обычно это архив формата.rar, заражающий при открытии устройство вирусом, который, в свою очередь, начинает заниматься бизнес-шпионажем, собирать корпоративные данные и отправлять на устройства киберпреступникам.

В последние годы наибольшую опасность представляет фишинг по способу распространения, получивший новые векторы развития:

— сайты-подделки, рассылаемые по электронной почте или в мессенджерах в форме письма или сообщения и отправляемые якобы от имени конкретной компании. Внутри они содержат замаскированную под документ таблицу или картинку, вредоносную программу, ссылку на созданный хакерами сайт, требование перевести деньги на указанный счет или по номеру телефона. Сотрудники компании-жертвы переходят по ссылке и указывают нужные данные, не замечая обмана. Например, в 2020 году в странах СНГ, в частности в Казахстане, рассылали письма от имени министра здравоохранения республики. Киберпреступники сообщали компаниям о возможности бесплатно получить защитные средства в рамках государственной помощи. Хозяйствующим субъектам необходимо было лишь заполнить приложенную анкету и отправить по обратному адресу. Во вложении письма находились документы, при запуске которых на компьютер попадала вредоносная программа из семейства Loki PWS, предназначенная для кражи логинов и паролей с зараженного компьютера;

— сайты-подделки, которые выдаются в поиске. Хакеры проявляют высокую активность накануне событий, связанных с потребительским или спортивно-массовым ажиотажем (старт продаж новых моделей iPhone, онлайн-распродажи, профессиональные праздники, спортивные мероприятия и др.), когда в преддверии корпоратива руководство

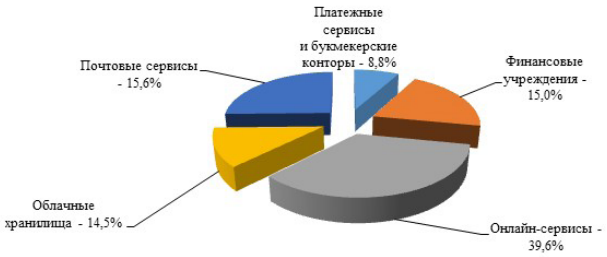

Рис. 2. Основные ресурсы, подделываемые хакерами при проведении фишинговых атак [6]

компаний, сотрудники или члены их семей совершают спонтанные интернет-покупки, принимают импульсивные и необдуманные решения в части расходов своего бюджета, не замечая при этом подвох. Так, в 2020 году накануне «черной пятницы» эксперты Group-IB обнаружили более 400 сайтов, копирующих маркетплейс AliExpress, 200 сайтов-клонов интернет-магазинов. При этом интернет-мошенники использовали похожие имена ресурсов, чтобы продавать подделки, контрафактный или низкокачественный товар, похищать данные банковских карт покупателей или заражать гаджеты пользователей вирусами.

Сегодня ключевая проблема, связанная с фишингом, заключается в том, что не существует ПО, которое защитило бы компанию и ее сотрудников. В конечном итоге все зависит от того, насколько они будут внимательны, распознают ли фейковые сайты, имитирующие интернет-страницы интернет-магазинов, стриминговых сервисов, социальных сетей. Хакеры рассчитывают на то, что руководство и персонал компании не заметят подделки и укажут на странице логины и пароли для входа в аккаунт на каком-либо сайте, номера карт, банковских счетов и другую конфиденциальную информацию.

Как свидетельствует бизнес-практика, чаще всего хакеры подделывают онлайн-сервисы, почтовые сервисы, финансовые учреждения, облачные хранилища, платежные сервисы и букмекерские конторы (рис. 2).

При проведении фишинговых атак хакеры даже могут шантажировать жертв и требовать деньги в обмен на то, что не станут публиковать данные в сети. Как отмечает директор департамента анализа защищенности и противодействия мошенничеству BI.ZONE Е. Волошин, в 2023 году хакерской группировкой Sneaking Leprechaun была придумана новая схема вымогательства, жертвами которой стали более 30 компаний России и Беларуси. Основная часть пострадавших бизнес-структур занимается разработкой и интеграцией программного обеспечения [7].

Группировка Sneaking Leprechaun, руководствуясь финансовыми мотивами, выбирает те компании, которые согласны платить за сохранность своих корпоративных данных. Жертвами ее фишинговых атак стали промышленные, логистические, финансовые и медицинские компании и даже государственные структуры. Киберпреступники группировки Sneaking Leprechaun для получения доступа к внутренним сетям российских и белорусских компаний воспользовались наличием уязвимостей в устаревших версиях Confluence, Bitrix и Webmin на серверах под управлением Linux. Они загружали свое вредоносное ПО и закреплялись в системе, получая необходимый доступ к конфиденциальным

данным корпораций. Оставаясь незамеченными, хакеры вручную анализировали данные и копировали те, которые считали ценными. В дальнейшем они шантажировали компании украденной у них информацией и требовали солидный выкуп, угрожая в противном случае разместить ее в открытом доступе.

Еще труднее сегодня компаниям бороться с многоэтапной фишинговой атакой Letscall, где современные технологии вишинга дополняются другими вредоносными инструментами

Вишинг (от англ. voice phishing — голосовой фишинг) — это разновидность мошенничества, при котором хакеры через телефонные звонки и голосовые сообщения принуждают персонал компании сообщить им конфиденциальные корпоративные данные, банковские реквизиты или совершить денежный перевод на их расчетный счет. В сочетании с ним вредоносное ПО распространяется через поддельный сайт, представляющий собой копию официального магазина приложений Google Play.

После установки такого ПО любой звонок из офиса компании может быть перенаправлен в мошеннический коллцентр, где участники киберпреступной группы в лице Android-разработчиков, бэкенд-мастеров и операторов звонков используют предварительно записанные сообщения-приманки и маршрутизацию голосового трафика. Подобная маршрутизация осуществляется за счёт IP-телефонии и WebRTC.

Также в арсенале хакеров протоколы Session Traversal Utilities for NAT и Traversal Using Relays around NAT. Все это дает возможность последним поддерживать качественную связь и обойти NAT-ограничения [8].

Не менее опасным для бизнес-деятельности компаний является *спуфинг* — новый тип кибератаки, в котором маскировка под легальный объект (компьютер, устройство или сеть) используется как средство проникновения в другие компьютерные сети. Это один из многих инструментов, используемый хакерами для доступа к компьютерам с целью получения конфиденциальных данных, превращения их в «зомби» (для злонамеренного использования) или запуска DoS-атак (атак типа «отказ в обслуживании»).

По своей сути, спуфинг выступает как техника фальсификации электронных данных киберпреступниками и искажения информации о себе. Например, они подделывают электронные адреса отправителей и другие параметры почты, чтобы скрыть истинное происхождение емэйла. Spoofed emails рассылаются для кражи личной или корпоративной информации, распространения вредоносных вложений и других хакерских атак.

К современным видам спуфинга относят:

— Email spoofing, позволяющий подделать истинный адрес отправителя письма и создать видимость, что оно пришло от другого лица. В поле «От кого» получатель такого сообщения увидит имя надёжного отправителя, хотя на самом деле им будет хакер;

— IP address spoofing — искажение IP-адресов в пакетах корпоративных данных, которые передаются целевому серверу. Данный вид используется, чтобы скрыть истинное местонахождение киберпреступника в интернете;

— DNS spoofing — подмена доменного имени (заполнение DNS-кеша поддельными данными) для перенаправления пользователя на ложный сайт. Целями этого вида может быть получение персональной информации или распространение вирусов;

— ARP spoofing — перехват и подмена данных, передаваемых между двумя устройствами;

— Caller ID spoofing — подмена номера телефона, в результате чего при входящем вызове на дисплее будет отображаться не тот номер, с которого на самом деле поступает звонок;

— GPS/GNSS spoofing — передача обманного сигнала GPS-приёмнику, применяемая для корректировки данных о фактической геолокации объекта в нужную хакеру сторону;

— Geolocation spoofing — подмена геолокации, заставляющая сеть считать, что устройство пользователя находится в другой стране (например, использование VPN-сервисов) [9].

Как новый тип атаки хакеров, направленной на компанию или совершающейся от её лица, спуфинг, на наш взгляд, вредит бизнесу по следующим причинам:

а) приводит к блокировкам IP и доменов. После рассылки спама эти IP-адреса попадают в чёрные списки;

б) снижает доставляемость, ибо из-за испорченной репутации отправителя фильтры блокируют легитимные письма. В свою очередь, массовые блокировки и низкая доставляемость приводят к ощутимым денежным потерям;

в) портит имидж бренда, поскольку, когда хакеры рассылают спам, фишинговые письма и вирусы от имени какой-либо компании, доверие клиентов к последней будет подорвано;

г) распространяет ПО для кражи внутренних и клиентских данных компании, что приводит к утечке конфиденциальной информации и тоже негативно скажется на репутации бренда.

Специалисты компании BI.ZONE предоставили статистику по борьбе с потенциально опасными рассылками по электронной почте. Выяснилось, что за первое полугодие 2023 года было заблокировано 600 тыс. нелегитимных электронных писем, в которых встречается спуфинг [10].

Разумеется, новым векторам развития киберпреступлений (модификациям фишинга, спуфингу, современным программам-вымогателям и др.) официальные органы в лице руководства страны, представителей Госдумы, Минцифры, Госкомнадзора, ФСТЭК, Росфинмониторинга пытаются всячески противостоять. Начнем с того, что укажем на подписание 13 июня 2023 г. Президентом России Федерального закона, предусматривающего конфискацию у киберпреступников имущества и денег, которые были получены в ходе противоправных действий. Изменения уже внесены в Уголовный кодекс, а закон обрёл юридическую силу. Среди других шагов, предпринятых на государственном уровне, следует, в первую очередь, выделить:

— подготовку Минцифры совместно с профильными ведомствами поправок для постановлений Правительства РФ № 325 и № 1236, касающихся реестра отечественного ПО, который функционирует уже более восьми лет. В частности, изменится перечень требований, необходимый для получения всех положенных льгот. Ожидается, что новые правила вступят в силу в 2024 году [11];

— внесение в Госдуму законопроекта группой политиков во главе с А. Немкиным о легализации «белых» хакеров (пентестеров), позволяющего последним вести свою деятельность законно при соблюдении определенных условий. Одним из глав-

ных условий законной работы пентестера является то, что результаты своей деятельность он обязан предоставить правообладателю в течение пяти дней [12];

— требование ФСТЭК к отечественным разработчикам софта ускорить исправления уязвимостей в ПО российского происхождения и пригрозила отзывом лицензий. В настоящее время они тратят в два раза больше времени на исправление ошибок, чем их зарубежные конкуренты, которым запрещено присутствие на рынке нашей страны [13];

— обеспокоенность Росфинмониторинга тем, что россияне всё чаще становятся дропперами, помогая злоумышленникам обналичивать украденные деньги. Дропперы — это подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт россиян. Наиболее распространённой схемой является оформление банковской карты и передача её третьим лицам за вознаграждение [14];

— одобренную Правительством РФ инициативу Минцифры о денежных компенсациях корпоративным и персональным пользователям, пострадавшим в результате утечки конфиденциальной информации. Такой шаг от компании будет рассматриваться в качестве смягчающего обстоятельства при определении наказания, предусмотренного законом об оборотных штрафах. Решать, достойна ли компания снисхождения, будут пострадавшие пользователи, которые могут отклонить компенсацию, если она их не устроит [15];

— введение государством новых правил кибербезопасности для хостинг-провайдеров. В рамках поправок к Закону «Об информации» они будут обязаны подключиться к системе противодействия кибератакам ФСБ ГосСОПКА, самостоятельно блокировать ресурсы, через которые ведутся кибератаки, и передавать данные о вредоносном трафике в систему. Также компаниям придется принимать участие в учениях по отключению рунета от глобальной сети [16].

При всей важности роли и места государства и его институтов в борьбе с киберпреступностью в РФ уже в 2023 году стало очевидным, что без участия отечественного бизнеса и населения страны проблему не решить. Сами по себе государственные меры поддержки и информационной защиты устраняют, скорее, последствия, а не причины высокой киберпреступности. Подобные «рамочные» условия обеспечения кибербезопасности, создаваемые государством, в известной степени ориентируют бизнес, особенно малый и средний, на использование лишь стратегий «удочерения» (умеренного партнерства) и «пассивной защиты» [17, 18].

Консолидированное участие российского бизнеса нашло свое выражение в создании акционерной компании F.C.C.T. Отделившись от Group-IB, она стала полностью отечественной с юридической и ресурсной точек зрения, а ее основой стали отечественные вендоры, заменившие западных.

Ключевыми направлениями деятельности компании F.C.C.T. на ИБ-рынке являются:

— поиск и сбор информации о нацеленных на определенную компанию кибератак, оптимизация существующих механизмов защиты от них с помощью данных киберразведки (Unified Risk Platform);

— проактивный анализ киберугроз, максимальная эффективность защиты и предотвращение хакерских атак благодаря пониманию методов, инструментов и намерений атакующих (Threat Intelligence);

— борьба с онлайн-мошенничеством; защита бизнеса и клиентов от всех видов цифровых рисков, предотвращение мошенничества в режиме реального времени и защита цифровой личности пользователя (Fraud Protection);

— выявление и устранение киберугроз; предотвращение атак в режиме реального времени для хостов, сети, инфраструктуры и электронной почты (Managed XDR);

— управление вектором кибератаки. Непрерывное обнаружение цифровых активов для устранения рисков и предотвращения утечек и инцидентов (Attak Surface Management);

— защита бренда и цифровых активов; AI-платформа для защиты цифровых активов, вашего бренда и клиентов, а также для идентификации и устранения цифровых рисков (Digital Risk Protection);

— блокировка хакерских атак в электронной почте; проактивное выявление и предотвращение сложных целевых атак в электронной почте с помощью запатентованной технологии защиты детонации любых вредоносных объектов в почте (Business Email Protection).

Уже первый год работы акционерной компании F.C.C.T., по мнению ее генерального директора В. В. Баулина, был успешным: число клиентов увеличилось на 1/3, объем продаж и выручка выросли на 60 % и 35 % соответственно. При этом 80 % выручки пришли в компанию через такой канал, как программа развития региональных партнеров [19].

Вместе с тем нельзя не отметить, что услуги, оказываемые хозяйствующим субъектам акционерной компании F.C.C.T., стоят по российским меркам недешево. Принимая во внимание существующую сегодня высокую дифференциацию отечественных компаний по размерам своих активов, следует признать, что многие средние и малые бизнес-структуры, особенно в регионах, не готовы к приобретению ИБ-услуг не только финансово, но и организационно [20]. До сих пор в лучшем случае ими делается один раз в год пентест, ни о какой-либо полной диагностике (check-up) разговор не ведется, явно не хватает квалифицированных кадров по противодействию киберугрозам и т.п.

Нами был изучен отраслевой ландшафт запроса представителей малых и средних форм хозяйствования юга Тюменской области на услуги поиска уязвимостей в ПО, веб-приложениях и IT-инфраструктуре компании (рис. 3).

Как видно из рис. 3, во всех рассмотренных отраслях запрос предпринимателей региона на услуги поиска уязвимостей в ПО, веб-приложениях и IT-инфраструктуре компании весьма невысокий и в среднем составляет примерно 11 %. По нашему мнению, дело не только в относительной дороговизне киберуслуг, но и в том, что на оказание последних не предусмотрено выделение финансовых средств из региональных программ поддержки малого и среднего бизнеса. Поэтому хозяйствующим субъектам «второго эшелона» приходится в этом вопросе рассчитывать только на собственные силы.

4. Заключение. В конце 2023 года в ряде регионов страны незначительный сегмент субъектов хозяйствования малого и среднего форматов начал инвестировать в развитие собственного ИБ-уровня. Речь идет о построении внутренних центров мо-

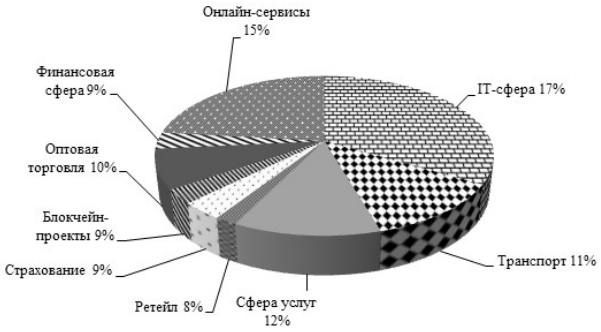

Рис. 3. Отраслевой ландшафт запроса предпринимателей юга Тюменской области на услуги поиска уязвимостей в ПО, веб-приложениях и IT-инфраструктуре компании

Рис. 4. Алгоритм достижения минимальных стандартов борьбы с киберпреступностью при построении типового SOC

ниторинга кибербезопасности (SOC — Security Operation Center), представляющих собой структурное подразделение компании, которое отвечает за оперативное изучение IT-среды и реагирования на киберинциденты.

Очевидно, что у бизнес-структур «второго эшелона» бюджеты достаточно скромные. Однако, на наш взгляд, их может оказаться достаточно для заложения основы построения типового SOC, удовлетворяющего самым минимальным стандартам борьбы с киберпреступностью. Алгоритм их достижения представлен нами в виде пошагового выполнения несложных организационно-методических рекомендаций по профилактике киберпреступлений и минимизации их последствий (рис. 4).

Шаг 1. Обнаружение, регистрация и классификация киберпреступлений является первым шагом на пути решения поставленной задачи. Для этого используются разные методы и инструменты подобной *идентификации*, в частности:

— мониторинг сетевого трафика, представляющий собой процесс наблюдения и анализа данных, передаваемых по сети, с целью выявления аномалий, подозрительных действий или нарушений политики кибербезопасности. Такой мониторинг осуществляется с помощью специализированного программного обеспечения или оборудования (снифферов, прокси-серверов, межсетевых экранов и пр.);

— экспресс-анализ журналов и протоколов, который можно рассматривать как процесс изучения и интерпретации записей, создаваемых информационными системами, приложениями или устройствами при выполнении различных операций, событий или действий. Он позволяет выявить киберпреступления, такие как неудачные попытки входа, несанкционированный доступ, изменение или удаление корпоративных, или персональных данных, нарушение правил доступа и др.;

— системы обнаружения и предотвращения вторжений (IDS/IPS) в виде программных или аппаратных решений, которые «мониторят» сетевой трафик, журналы и протоколы, сравнивают их с базой данных угроз, уязвимостей или поведенческих моделей. Системы обнаружения вторжений (IDS) предназначены для оповещения руководства компании о киберпреступлениях, их блокировке или приостановке. Добавим, что системы IDS/IPS могут быть развернуты на разных уровнях сети (например, хост, сетевой уровень, прикладной уровень).

Шаг 2. Системный подход в борьбе с киберпреступлениями требует четкого выполнения согласованных *процедур реагирования*, которые определяют, как действовать в случае их обнаружения. Процедуры реагирования на киберпреступления включают в себя:

— процесс создания документа, который содержит цели, политики, роли, обязанности, процессы и ресурсы, необходимые для реагирования на киберпреступления и который заканчивается составлением плана реагирования. Он должен быть разработан заранее, с учетом различных сценариев, угроз, уязвимостей, а также регулярно обновляться и тестироваться;

— процесс оповещения и координации заинтересованных сторон (менеджмент компании, ее персонал, клиенты, партнеры, поставщики, правоохранительные органы и т.д.) при обнаружении киберпреступления и о его характеристиках, таких как время, место, источник, цель, вектор, эффект и др. Данные сообщения также включают в себя анализ, оценку, приоритеты, назначение, исполнение и контроль действий, направленных на предотвращение киберпреступлений и их последствий;

— процесс возвращения информации и информационных систем к нормальному состоянию после киберпреступления, выяснения причин, деталей и ранга его значимости. Также сюда относится разработка предложений и выводов, направленных на профилактику киберпреступлений и понесенного из-за них материального и финансового ущерба.

Шаг 3. Превентивные меры по предотвращению киберпреступлений и минимизации их последствий включают в себя следующие действия:

— процесс обучения и информирования сотрудников компании, ее клиентов и бизнес-партнеров о принципах, политике, стандартах и практиках кибербезопасности, о типах, методах и последствиях риск-событий и пр. Обучение персонала и повышение осведомленности о возможных киберпреступлениях может быть осуществлено с помощью различных форм и методов (лекций, семинаров, вебинаров, тренингов, брошюр, плакатов, электронных писем и др.);

— процесс создания и внедрения политики кибербезопасности, применения набора правил, руководств, процедур и стандартов, которые определяют, как информация и информационные системы должны быть защищены, использованы, управляемы и поддерживаемы. Киберполитика компании должна быть основана на анализе предпринимательских рисков, согласована с бизнес-целями и требованиями, должна соблюдаться всеми заинте-

ресованными сторонами, а также документирована, распространена, контролируема, обновляема;

— процесс проверки состояния и оценки эффективности кибербезопасности, выявления и устранения угроз и уязвимостей, нарушений в информационных системах. Регулярные аудиты риск-событий, их последствий могут быть проведены как специалистами самой компании, так и на основе аутстаффинга с применением разнообразных методик и инструментов (например, тестирования, сканирования, наблюдения, интервью, анкетирования и т.д.

Шаг 4. Продолжающееся расширение спектра киберугроз, векторов хакерских атак и утечек корпоративных и персональных данных свидетельствует о том, что в настоящее время одних лишь превентивных мер по предотвращению киберпреступлений и минимизации их последствий явно недостаточно. Объективно необходимым становится развитие современных технологий, сервисов, приложений и устройств обнаружения и предотвращения киберпреступлений. Так, блокчейн и криптография могут быть использованы для создания защищенных систем хранения, передачи и проверки конфиденциальных данных компании и ее работников. Биометрия и поведенческая аналитика способны усилить аутентификацию и авторизацию пользователей, а также обнаружить потенциальные угрозы и уязвимости, а значит, предотвратить киберпреступления. Применение квантовых вычислений и квантовой криптографии способствует созданию более надежных систем шифрования и дешифрования корпоративных и персональных данных.

Что касается искусственного интеллекта (AI) и машинного обучения (ML), то сегодня они являются одними из самых перспективных и влиятельных технологий в области кибербезопасности. Благодаря им становится возможным анализ больших объемов коммерческих данных, выявление аномалий, обучение нормальному и аномальному бизнес-поведению, автоматизация и оптимизация процессов реагирования на киберпреступления и пр. Заключительный четвертый шаг предложенного алгоритма выходит за рамки минимальных стандартов борьбы с киберпреступностью на уровне малых и средних компаний. Но гипотетически его допуская, мы прописываем траекторию стратегии развития типового SOC от начала до превращения в завершенную социально-экономическую систему.

Библиографический список

1. Россия вошла в топ-10 по количеству кибератак // Инфобезопасность. URL: https://infobezopasnost.ru/blog/news/rossiya-voshla-v-top-10-po-kolichestvu-kiberatak/ (дата обращения: 05.07.2023).

2. Российские компании озаботились своей безопасностью // Cisoclub. URL: https://cisoclub.ru/rossijskie-kompanii-ozabotilis-svoej-bezopasnostju/ (дата обращения: 31.05.2023).

3. Россия вошла в десятку самых атакуемых хакерами стран мира // Lenta.ru URL: https://lenta.ru/news/2023/07/05/ddos/ (дата обращения: 05.07.2023).

4. Волк И. В России за полгода почти на 30 % выросло число киберпреступлений // ТАСС. URL: https://tass.ru/obschestvo/18322395 (дата обращения: 20.07.2023).

5. Литвинов Р. Количество фишинга возросло почти в 5 раз // Инфобезопасность. URL: https://infobezopasnost.ru/blog/news/kolichestvo-fishinga-vozroslo-pochti-v-5-raz/ (дата обращения: 12.07.2023).

6. Марков Д. Что такое фишинг: как не стать жертвой хакеров // РБК. Тренды. URL: https://trends.rbc.ru/trends/industry/602e9fe79a7947a4bd611504 (дата обращения: 07.02.2023).

7. Волошин Е. BI.ZONE обнаружила необычные атаки вымогателей на десятки компаний в России и Беларуси // BI.ZONE. URL: https://bi.zone/news/bi-zone-obnaruzhila-neobychnye-ataki-vymogateley-na-desyatki-kompaniy-v-rossii-i-belarusi/?s_phrase_id=3649 (дата обращения: 23.05.2023).

8. Letscall new sophisticated Vishing toolset // Threat Fabric. URL: https://www.threatfabric.com/blogs/letscall-new-sophisticated-vishing-toolset (дата обращения: 07.07.2023).

9. Актуальные методы спуфинга в наши дни // Хакер. URL: Хакер.ru/2023/10/16/ relevant-spuffing/ (дата обращения: 07.07.2023).

10. Меджлумов М. 75 % входящих писем представляют опасность для российских компаний // Инфобезопасность. URL: https://infobezopasnost.ru/blog/news/ (дата обращения: 25.07.2023).

11. Любавина А. Реестр отечественного ПО разделят на российский софт первого и второго сорта // CNEWS. URL: https://www.cnews.ru/news/top/2023-12-04_pravila_vneseniya_v_reestr (дата обращения: 04.12.2023).

12. В Госдуму внесли проект о легализации «белых» хакеров // РИА Новости. URL: https://ria.ru/20231212/zakonoproekt-1915369737.html (дата обращения: 12.12.2023).

13. Защиты не напасешься // Коммерсантъ. URL: https://www.kommersant.ru/doc/6266589?query=%D0%97%D0%B0%D1%89%D0%B8%D1%82%D1%8B%20%D0%BD%D0%B5%20%D0%BD%D0%B0%D0%BF%D0%B0%D1%81%D0%B5%D1%88%D1%8C%D1%81%D1%8F (дата обращения: 10.10.2023).

14. Росфинмониторинг: многие граждане не осознают, что мошенники делают их соучастниками преступлений // Cisoclub. URL: https://cisoclub.ru/rosfinmonitoring-mnogie-grazhdane-ne-osoznajut-chto-moshenniki-delajut-ih-souchastnikami-prestuplenij/ (дата обращения: 02.11.2023)

15. Литвинов Р. Пользователям возместят ущерб за утечки информации // Инфобезопасность. URL: https://infobezopasnost.ru/blog/news/polzovatelyam-vozmestyat-ushherb-za-utechki-informatsii/ (дата обращения: 26.09.2023).

16. Провайдеров готовят к отключениям // Коммерсантъ. URL: https://www.kommersant.ru/doc/6212718?query=%D0%9F%D1%80%D0%BE%D0%B2%D0%B0%D0%B9%D0%B4%D0%B5%D1%80%D0%BE%D0%B2%20%D0%B3%D0%BE%D1%82%D0%BE%D0%B2%D1%8F%D1%82%20%D0%BA%20%D0%BE%D1%82%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BD%D0%B8%D1%8F%D0%BC (дата обращения: 15.09.2023).

17. Simonov S. G., Lysenko I. V., Khamatkhanova M. A. Approaches to the assessment of economic security of subjects small and medium business in the Eurasian economic union // Mediterranean Journal of Social Sciences. 2015. Vol. 6, no. 4. P. 509–515. DOI: 10.5901/mjss.2015.v6n4p509.

18. Симонов С. Г., Курушина Е. В., Корякина Е. А. Бизнес в эпоху глобальных перемен: моногр. Тюмень: Изд-во ТИУ. 2023. 213 с. EDN: GSGWJI.

19. Шабанов И. Валерий Баулин: Акционеры F.A.S.S.T. видят огромный потенциал развития в России // Anti-malware. URL: https://www.anti-malware.ru/interviews/2023-07-14/41565 (дата обращения: 14.07.2023).

20. Симонов С. Г., Руднева Л. Н., Корякина Е. А. Средний и малый бизнес Тюменской области: сущность, становление, современные тенденции развития: моногр. Тюмень: Изд-во ТИУ. 2020. 196 с. ISBN 978-5-9961-2445-9.

СИМОНОВ Сергей Геннадьевич, доктор социологических наук, кандидат экономических наук, профессор кафедры экономики и организации произ-

водства Тюменского индустриального университета (ТИУ), г. Тюмень.
SPIN-код: 7421-8418
AuthorID (РИНЦ): 435655
Адрес для переписки: v.simonova.67@mail.ru
ЛЫСЕНКО Игорь Вячеславович, кандидат экономических наук, доцент кафедры технологии машиностроения ТИУ, г. Тюмень.
SPIN-код: 3356-4948
AuthorID (РИНЦ): 718473
Адрес для переписки: lysenkoiv@tyuiu.ru

Для цитирования

Симонов С. Г., Лысенко И. В. Российский бизнес в условиях роста киберпреступности: изменения экономического поведения и защитные механизмы // Омский научный вестник. Сер. Общество. История. Современность. 2024. Т. 9, № 3. С. 141—149. DOI: 10.25206/2542-0488-2024-9-3-149-157.

Статья поступила в редакцию 22.03.2024 г.

UDC 394:314.15
DOI: 10.25206/2542-0488-2024-9-3-149-157
EDN: NMIBGA

S. G. SIMONOV
I. V. LYSENKO

Industrial University of Tyumen,
Tyumen, Russia

RUSSIAN BUSINESS IN THE CONTEXT OF THE GROWTH OF CYBERCRIME: CHANGES IN ECONOMIC BEHAVIOR AND PROTECTIVE MECHANISMS

The article is devoted to the identification and analysis of new vectors of cybercrime development, their localization and prevention. The analysis of secondary data, questionnaires, and expert assessment are used as research methods for this problem. The statistics of cybercrime in foreign countries and Russia in recent years have been analyzed. It is found out how the domestic business has changed its attitude to the security of information and information systems of the company. The sectoral landscape of cybercrimes in the Russian Federation for 2023 is presented. New vectors of phishing development are considered in detail and the main resources forged by hackers during phishing attacks are identified. Special attention is paid to phishing by the method of distribution, which today poses the greatest danger to Russian companies. Spoofing has been studied as a new type of cyberattack, where masquerading as a legal object (computer, device or network) is used by hackers as a means of penetrating other computer networks. The characteristics of modern types of spoofing and the negative consequences for business that they lead to are given. The measures taken at the state level to counter new vectors of cybercrime development are indicated. The conclusion is substantiated that state support and information protection measures themselves eliminate the consequences rather than the causes of high cybercrime, which is why the security problem cannot be solved without the participation of domestic business and the population of the country. The consolidated participation of Russian business in the fight against cybercrime is noted, which found its concrete embodiment in the creation of the F.C.C.T. joint-stock company. The key areas of activity of this company in the information technology market and the results of its work in 2023 are highlighted. Attention is focused on the fact that the creation of a joint-stock company F.C.C.T. in the country does not fully solve the problem of ensuring information security, which primarily concerns small and medium-sized business structures. It is stated that many of them, especially in the Russian regions, are not ready to purchase information security services not only financially, but also organizationally. Due to the low demand of entrepreneurs for vulnerability search services in the company's software, web applications and IT infrastructure, it is proposed to build a typical SOC that meets the most minimal standards for combating cybercrime. An algorithm has been developed to achieve them in the form of step-by-step implementation of simple organizational and methodological recommendations for the prevention of cybercrimes and minimizing their consequences for small and medium-sized businesses.

Keywords: cybercrime, phishing, spoofing, hacker attack, information security, cyber threats and vulnerabilities, small and medium-sized businesses.

References

1. Rossiya voshla v top-10 po kolichestvu kiberatak [Russia ranks in the top 10 in the number of cyberattacks] // Infobezopasnost'. *Infosecurity News.* URL: https://infobezopasnost.ru/blog/news/rossiya-voshla-v-top-10-po-kolichestvu-kiberatak/ (accessed: 05.07.2023). (In Russ.).

2. Rossiyskiye kompanii ozabotilis' svoyey bezopasnost'yu [Russian companies are concerned about their used danger] // Cisoclub. *Cisoclub.* URL: https://cisoclub.ru/rossijskie-kompanii-ozabotilis-svoej-bezopasnostju/ (accessed: 31.05.2023). (In Russ.).

3. Rossiya voshla v desyatku samykh atakuyemykh khakerami stran mira [Russia is among the top ten countries most attacked by hackers in the world] // Lenta.ru. *Lenta.ru.* URL: https://lenta.ru/news/2023/07/05/ddos/ (accessed: 05.07.2023). (In Russ.).

4. Volk I. V Rossii za polgoda pochti na 30 % vyroslo chislo kiberprestupleniy [In Russia, the number of cybercrimes has increased by almost 30 % in six months] // TASS. *TASS.* URL: https://tass.ru/obschestvo/18322395 (accessed: 20.07.2023). (In Russ.).

5. Litvinov R. Kolichestvo fishinga vozroslo pochti v 5 raz [The amount of phishing has increased almost 5 times] // Infobezopasnost'. *Infosecurity News.* URL: https://infobezopasnost.ru/blog/news/kolichestvo-fishinga-vozroslo-pochti-v-5-raz/ (accessed: 12.07.2023). (In Russ.).

6. Markov D. Chto takoye fishing: kak ne stat' zhertvoy khakerov [What is phishing: how to avoid becoming a victim of hackers] // RBK. Trendy. *RBC. Trends.* URL: https://trends.rbc.ru/trends/industry/602e9fe79a7947a4bd611504 (accessed: 07.02.2023). (In Russ.).

7. Voloshin E. BI.ZONE obnaruzhila neobychnyye ataki vymogateley na desyatki kompaniy v Rossii i Belarusi [BI.ZONE discovered unusual ransomware attacks on dozens of companies in Russia and Belarus] // BI.ZONE. *BI.ZONE.* URL: https://bi.zone/news/bi-zone-obnaruzhila-neobychnye-ataki-vymogateley-na-desyatki-kompaniy-v-rossii-i-belarusi/?s_phrase_id=3649 (accessed: 23.05.2023). (In Russ.).

8. Letscall new sophisticated Vishing toolset // Threat Fabric. URL: https://www.threatfabric.com/blogs/letscall-new-sophisticated-vishing-toolset (accessed: 07.07.2023). (In Engl.).

9. Aktual'nyye metody spufinga v nashi dni [Current spoofing methods today] // Xakep. *Xakep.* URL: Khaker.ru/2023/10/16/relevant-spuffing/ (accessed: 07.07.2023). (In Russ.).

10. Medzhlumov M. 75 % vkhodyashchikh pisem predstavlyayut opasnost' dlya rossiyskikh kompaniy [75 % of incoming emails pose a threat to Russian companies] // Infobezopasnost'. *Infosecurity News.* URL: https://infobezopasnost.ru/blog/news/ (accessed: 25.07.2023). (In Russ.).

11. Lyubavina A. Reyestr otechestvennogo PO razdelyat na rossiyskiy soft pervogo i vtorogo sorta [The register of domestic software will be divided into Russian software of the first and second grade] // CNEWS. *CNEWS.* URL: https://www.cnews.ru/news/top/2023-12-04_pravila_vneseniya_v_reestr (accessed: 04.12.2023). (In Russ.).

12. V Gosdumu vnesli proyekt o legalizatsii «belykh» khakerov [A draft law on the legalization of «white hat» hackers has been submitted to the State Duma] // RIA Novosti. *RIA Novosti.* URL: https://ria.ru/20231212/zakonoproekt-1915369737.html (accessed: 12.12.2023). (In Russ.).

13. Zashchity ne napasesh'sya [You can't get enough protection] // Kommersant". *Kommersant.* URL: https://www.kommersant.ru/doc/6266589?query=Zashchity ne napasesh'sya (accessed: 10.10.2023). (In Russ.).

14. Rosfinmonitoring: mnogiye grazhdane ne osoznayut, chto moshenniki delayut ikh souchastnikami prestupleniy [Rosfinmonitoring: many citizens do not realize that scammers make them accomplices in crimes] // Cisoclub. *Cisoclub.* URL: https://cisoclub.ru/rosfinmonitoring-mnogie-grazhdane-ne-osoznajut-chto-moshenniki-delajut-ih-souchastnikami-prestuplenij/ (accessed: 02.11.2023). (In Russ.).

15. Litvinov R. Pol'zovatelyam vozmestyat ushcherb za utechki informatsii [Users will be compensated for damages for information leaks] // Infobezopasnost'. *Infosecurity News.* URL: https://infobezopasnost.ru/blog/news/polzovatelyam-vozmestyat-ushherb-za-utechki-informatsii/ (accessed: 26.09.2023). (In Russ.).

16. Provayderov gotovyat k otklyucheniyam [Providers are preparing for shutdowns] // Kommersant". *Kommersant.* URL: https://www.kommersant.ru/doc/6212718?query=Provayderov gotovyat k otklyucheniyam (accessed: 15.09.2023). (In Russ.).

17. Simonov S. G., Lysenko I. V., Khamatkhanova M. A. Approaches to the assessment of economic security of subjects small and medium business in the Eurasian economic union // Mediterranean Journal of Social Sciences. 2015. Vol. 6, no. 4. P. 509–515. DOI: 10.5901/mjss.2015.v6n4p509. (In Engl.).

18. Simonov S. G., Kurushina E. V., Koryakina E. A. Biznes v epokhu global'nykh peremen [Business in an era of global change]. Tyumen, 2023. 213 p. EDN: GSGWJI. (In Russ.).

19. Shabanov I. Valeriy Baulin: Aktsionery F.A.S.S.T. vidyat ogromnyy potentsial razvitiya v Rossii [Valery Baulin: Shareholders of F.A.S.S.T. see huge development potential in Russia] // Anti-malware. *Anti-malware.* URL: https://www.anti-malware.ru/interviews/2023-07-14/41565 (accessed: 14.07.2023). (In Russ.).

20. Simonov S. G., Rudneva L. N., Koryakina E. A. Sredniy i malyy biznes Tyumenskoy oblasti: sushchnost', stanovleniye, sovremennyye tendentsii razvitiya [Medium and small business of the Tyumen region: essence, formation, modern development trends]. Tyumen, 2020. 196 p. ISBN 978-5-9961-2445-9.). (In Russ.).

SIMONOV Sergey Gennadievich, Doctor of Social Sciences, Candidate of Economic Sciences, Professor of Economics and Production Organization Department, Industrial University of Tyumen (IUT), Tyumen.
SPIN-code: 7421-8418
AuthorID (RSCI): 435655
Correspondence address: v.simonova.67@mail.ru
LYSENKO Igor Vyacheslavovich, Candidate of Economic Sciences, Associate Professor of Mechanical Engineering Technology Department, IUT, Tyumen.
SPIN-code: 3356-4948
AuthorID (RSCI): 718473
Correspondence address: lysenkoiv@tyuiu.ru

For citations

Simonov S. G., Lysenko I. V. Russian business in the context of the growth of cybercrime: changes in economic behavior and protective mechanisms // Omsk Scientific Bulletin. Series Society. History. Modernity. 2024. Vol. 9, no. 3. P. 149–157. DOI: 10.25206/2542-0488-2024-9-3-149-157.

Received March 22, 2024.