рабочих, наоборот, сократилось с 64,9 до 52,9 тыс. чел. Это говорит о том, что повышается квалификационный уровень работников ПАО «Транснефть».

- Преобладают работники, имеющие стаж работы свыше 5 лет, – и этот процент вырос за 5 лет с 68% до 69%, что говорит об устойчивом развитии персонала. Что же касается возрастной структуры, то за 5 лет наметилась позитивная динамика: процент молодежи до 30 лет остался на уровне 19%, но процент старшего возраста свыше 50 лет уменьшился с 20,9% до 19,5%. Такая динамика говорит о постепенном омоложении трудового коллектива.

- Абсолютное большинство работников (93%) постоянно проходят обучение. Обучение направлено как на подтверждение, так и на повышение квалификации, а также оно проводится с целью освоения компетенций конкретной производственной деятельностью.

В ПАО «Транснефть» в системе управления персоналом выявлены следующие проблемы:

1. Коэффициент текучести кадров достаточно высокий (более 10%). Из 128 человек, уволившихся за календарный год, 16 – руководители, 27 – специалисты, 85 – рабочие.

2. При широком охвате обучающихся динамика повышения уровня квалификации специалистов и работников не успевает за сменой самих кадров при достаточно высокой текучести для данного типа предприятия.

3. Недостаточно эффективная работа по управлению персоналом, недостаток кадров в ней, не используются возможности Интернета.

Проблемы повышения эффективности системы управления персоналом предлагается решить в следующих направлениях:

1. Разработка программы адаптации для вновь принятых молодых специалистов. Данная программа должна быть направлена на долгосрочное закрепление молодых специалистов посредством формирования приверженности и трансляции корпоративной культуры в удаленные регионы.

2. Совершенствование автоматизации системы управления персоналом, что позволит ускорить бизнес-процессы управления персоналом и, соответственно, приведет к ускорению принятия управленческих решений.

3. Переориентация договоров о сотрудничестве и дополнительной переподготовке с высшими учебными заведениями. территориально расположенными поблизости от структурных подразделений предприятия.

Список источников:

1. Волкова Е.В. Значимость внедрения эффективной системы адаптации работников в российских компаниях / Е.В. Волкова, Е.А. Багрова // Общество, государство, личность: молодежное предпринимательство в поведенческой экономике в условиях цифровизации: Материалы XXI Междунар. научно-практ. конф. студентов, магистрантов, аспирантов и молодых ученых. - Казань, 29 апр. 2021 г. - Казань: ИЦ Университета управления «ТИСБИ», 2021. - С. 134-137.

2. Макринова Е.И., Трунова С.Е., Лавренова Е.В. Системная методология управления персоналом и формирования кадровой базы организаций в концепте экономики знаний // Фундаментальные исследования. - 2018. - № 6-1. - С. 154-160.

3. Селентьева Д.О., Зиганшина Д.Г. Совершенствование системы управления персоналом // Междунар. ж-л гуманит. и естеств. наук. - 2018. - № 4. - С. 27-32.

ТИПОЛОГИЧЕСКИЕ ОСОБЕННОСТИ КИБЕРПРЕСТУПНИКОВ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ И ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Айнутдинова К.А., *канд. юрид. наук, магистр психологии, доцент,*
Университет управления «ТИСБИ», г. Казань;
Айнутдинова И.Н., *д-р пед. наук, профессор,*
Казанский (Приволжский) федеральный университет

Аннотация. Цель статьи - определить и сформулировать типологические особенности киберпреступников в условиях глобализации и цифровизации экономики; вычленить компоненты экосистемы киберпреступности; описать группы киберпреступников; установить их преступные мотивы и средства атаки.

Ключевые слова: глобализация, цифровизация, экосистема, киберпреступность, киберпреступник.

Интерес к теме исследования вызван колоссальными негативными изменениями, происходящими сегодня в экосистеме киберпреступности, которая в условиях глобализации и цифровизации экономики демонстрирует не только тенденцию к расширению географии и ландшафта, но и порождает наращивание и усложнение функций и ролей всех своих неотъемлемых компонентов, включая технологическую инфраструктуру, инструменты для атак и разнообразные паттерны поведения потенциальных участников криминальной деятельности [1]. Экосистема киберпреступности оперативно реагирует на глобальные вызовы эпохи и искусно включает в свою структуру и сферу преступного воздействия ключевые, с точки зрения экономистов, элементы цифровой экономики, а именно: инновационное аппаратное и программное обеспечение; разветвленные сети связи (инфраструктуру); цифровые процессы, обеспечивающие ведение бизнеса; рынки электронной коммерции для продажи товаров посредством сети Интернет; цифровизацию банковского сектора для оптимизации финансовых транзакций и платежей, включая блокчейн-технологии и криптовалюты, и пр. [2].

Отметим, что уровень цифровизации экономики в современных условиях достаточно высок и коррелирует с ее массовостью и охватом

практически всех сфер жизни людей, что опять же не ускользает от внимания киберпреступников. При этом, если Национальная программа «Цифровая экономика РФ» [3] одной из своих приоритетных задач видит улучшение жизни людей и максимальное удовлетворение их потребностей за счет использования современных цифровых технологий, безопасного доступа к информации и электронным сервисам, то киберпреступники, напротив, действуют в сети Интернет варварски, с целью нанесения материального и морального ущерба пользователям через взломы компьютерных сетей, кражи данных, мошенничество, вымогательство и иные киберпреступления, часто совершаемые ими для получения финансовой выгоды.

По данным статистических наблюдений и ведомственных отчетов МВД и Прокуратуры РФ, регулярно публикуемых на Портале правовой статистики [4], в январе-феврале текущего года в ряде российских регионов было отмечено незначительное снижение (на 2,1%) общего количества зарегистрированных преступлений (149,5 тыс.), а тяжких и особо тяжких преступлений – на 4,3% по сравнению с тем же периодом прошлого года. При этом отмечен рост (+4%) преступлений в сфере IT-технологий или компьютерной информации, и на эти деяния (38,7 тыс.) приходится каждое из четырех регистрируемых преступлений. Большинство из них (74%) совершено с использованием сети Интернет (+18,1%) – 27,1 тыс. и/или при помощи средств мобильной связи (+7,2%) – 15,7 тыс. [4].

В некоторых регионах отмечена положительная динамика снижения числа краж с банковских счетов или в отношении электронных денежных средств на 18,6% (9,6 тыс.), а также мошенничеств, совершенных в сфере IT-технологий или компьютерной информации на 9% (27 тыс.). При этом ситуация в крупных городах и развитых регионах выглядит не столь радужно. Наибольшее число таких деяний (+39 %) – 16 тыс. зарегистрировано в г. Москва – 995, Республике Татарстан – 353 и г. Санкт-Петербург – 351 [4]. Эти показатели, вероятно, связаны с рядом социально-экономических факторов, например, более развитой инфраструктурой крупных городов, сосредоточением банков, бизнес-компаний и иных финансовых организаций, высокими доходами населения, повсеместным распространением широкополосного Интернета, доступностью цифровых услуг и сервисов, расширением рынка электронных услуг для населения и др.

Задача, стоявшая перед авторами, заключалась в изучении типологических особенностей лиц, совершающих киберпреступления в условиях глобализации и цифровой трансформации общества. В первую очередь, нас интересовала их роль в преступных деяниях как компонента экосистемы киберпреступности. Мы исходили из того, что знание типологических особенностей преступников позволит уяснить выбор ими мотивов и средств совершения киберпреступления, а также поможет специалистам при разработке стратегий противодействия им.

Анализ отечественной и зарубежной литературы по теме вкупе с данными статистики позволяют выделить типологические особенности, присущие лицам, совершающим киберпреступления с целью причинения различных видов ущерба либо отдельным гражданам и организациям, либо целым государствам и даже международному сообществу [5-7]. Практически всеми ими движет корыстное побуждение, направленное на извлечение имущественной выгоды, и эгоизм, что проявляется в том, что большинство преступников ставят собственное личное материальное и моральное благополучие выше закона и интересов других лиц [5].

Демографические особенности киберпреступников зеркально отображают обычный уголовный мир в том смысле, что в этой среде процент женщин очень мал и преобладают лица мужского пола в возрасте от 16 до 50 лет. Однако, по данным Управления ООН по наркотикам и преступности (UNODC), в последние годы в России отмечается расширение возрастных границ киберпреступности: во-первых, за счет вовлечения молодежи поколения Z, исповедующей с раннего подросткового возраста (12-14 лет) субкультуру свободного от запретов сетевого пространства, в том числе для совершения краж и финансового мошенничества в сети Интернет; во-вторых, за счет увеличения числа пожилых лиц (60 лет и более), в особенности, когда киберпреступления связаны с детской порнографией или «грумингом» – созданием доверительных отношений онлайн с ребенком/подростком с целью его сексуальной эксплуатации или насилия [6].

Высокий уровень образования (особенно в сфере компьютерных наук) отмечается лишь у определенной части преступников, при этом многие из установленных преступников не имеют специальной подготовки для работы со сложными программами или сетевыми ресурсами, а действуют «по наитию». Киберпреступникам все реже требуются сложные навыки или оборудование в связи с появлением и доступностью различных вредоносных инструментариев. Многие хакеры отмечают, что «искусственно» приобрели технические навыки при работе с таким вредоносным компьютерным инструментарием, как «ZeuS» или «Butterfly Bot» [6]. При этом было бы ошибочно думать о заведомо низком уровне IT-компетентности современных хакеров, особенно в свете усложнения архитектуры компьютерных систем, обновления программного обеспечения и расширения сфер организованной преступной деятельности [7]. По мнению О.А. Пучкова, для описания хакера понадобится много иных навыков, умений и личностных качеств, характеризующих его криминальный профессионализм [7].

С учетом приведенных выше особенностей рассмотрим некоторые группы преступников для формирования более полного представления об экосистеме киберпреступности. К первой группе отнесем так называемых «бездельников» (*scamps*), которые с раннего детства демонстрируют модель делинквентного поведения и либо из любопытства, либо из хулиганских

побуждений взламывают компьютерные сети, внедряют вирусы и черви через почтовые отправления, распространяют музыку или фильмы, защищенные авторским правом, и пр. Делают они это на первых порах, в основном, чтобы самоутвердиться перед сверстниками и показать свое «бесстрашие» перед законом. По мнению экспертов, *scamps* привычно совершают киберпреступления и во взрослой жизни, часто входят в категорию лиц без образования, с низким уровнем дохода или не имеющих устойчивого источника дохода и/или без постоянного места работы [5].

Вторая группа условно называется «детвора, балующаяся скриптами» (*script kiddies*). Это хакеры-подражатели – дети и подростки в возрасте от 6 до 18 лет, которые мечтают быть полноценными хакерами, но не имеют до поры до времени серьезных технических навыков и знаний. Именно они с малых лет исповедует субкультуру свободного Интернета и без особых угрызений совести используют вредоносные программы для атак на сети и веб-сайты. Обычно они атакуют лишь слабозащищенные системы и довольствуются малой наживой.

К следующей группе отнесем многочисленных «вредителей» или «авторов вредоносных программ» (*malware authors*), которые демонстрируют сочетание профессионализма и фанатизма в области компьютерного программирования. Обычно их действия носят спонтанный характер, а противоправные намерения формируются в конкретной ситуации, которая, как им кажется, служит вызовом их профессиональным и интеллектуальным способностям; таким «триггером» может стать повышение мер по обеспечению компьютерной безопасности банка. Не имея изначально четких корыстных намерений, «вредитель» может запросить в процессе выкуп за действие/бездействие по заражению сторонней системы [8].

Наибольшую опасность представляет группа «профессиональных хакеров и взломщиков» (*professional hackers*), которых мотивируют только деньги. Эта группа киберпреступников наносит наибольший финансовый и репутационный ущерб, чем все другие группы вместе взятые [6]. Профессиональные хакеры создают продвинутые вредоносные инструменты, посредством которых атакуют правительственные и финансовые учреждения, сайты электронной коммерции, включая онлайн-продажи, Интернет-банкинг, платежные системы и т.д. Следует различать белых хакеров (специалистов высокого уровня, нанимаемых банками и предприятиями для установления и ликвидации сетевых уязвимостей); серых хакеров (больше похожих по своей импульсивности на «вредителей») и самых корыстных, зловредных и опасных черных хакеров, которые, в свою очередь, подразделяются на «взломщиков» (*crackers*), работающих с системами защиты компьютерной информации; «мошенников» (*phreakers*), специализирующихся на получении доступа к защищенным каналам связи и коммуникаций с целью совершения кражи, порчи или блокировки данных; и «кибертеррористов» (*cyberterrorists*),

осуществляющих массированные атаки в целях запугивания населения или принуждения власти к совершению определенных действий [5; 6].

В эпоху цифровой трансформации значительные угрозы также исходят от «инсайдеров» (*insiders*), или сотрудников, обладающих специальными знаниями и доступом к конфиденциальной и/или эксклюзивной информации о деятельности компании или корпорации [6]. Эти злоумышленники считаются крайне опасными. В силу своего служебного положения они могут нанести до 80% урона путем промышленного шпионажа или раскрытия торговых секретов.

Подводя итоги проведенному исследованию, резюмируем, что глобальные технологические процессы и цифровая трансформация экономики оказывают беспрецедентное влияние на все сферы жизни общества. При общем снижении преступности в стране преступления в сфере IT-технологий или компьютерной информации по-прежнему показывают рост в некоторых крупных городах и регионах, а экосистема киберпреступности развивается и совершенствуется, часто копирует лучшие элементы цифровой экономики или даже мимикрирует под нее. Постоянно обновляемая технологическая инфраструктура, все более изощренные и технологичные инструменты для атак и способы сокрытия следов киберпреступлений дополняются новыми паттернами поведения участников криминальной деятельности. Это меняет и расширяет традиционный стереотип образа киберпреступника и позволяет рассматривать злоумышленников, обладающих типологическими особенностями, но функционирующих в единой экосистеме киберпреступности, с позиции их мотивов и потенциальных средств совершения киберпреступлений. Такие знания должны помочь специалистам при разработке стратегии и тактики противодействия киберпреступности.

Список источников:

1. Keck M., et al. (2022). The role of cybersecurity and data security in the digital economy: Brief / M. Keck, S. Gillani, A. Dermish, J. Grossman. - UNCDF Publishing: Policy Accelerator. - 22 p.

2. Gritzalis D. (2013). Cybercrime in the Digital Economy: Editorial / Dimitris Gritzalis. Computers & Security, 38. - P. 1-2.

3. Волкова А.А., Плотникова В.А., Рукинов М.В. Цифровая экономика: сущность явления, проблемы и риски формирования и развития // Власть и экономика. - 2019. - № 4. - С. 38-49.

4. Состояние преступности в России за январь-февраль 2022 г. / Ежемесячный сб. о состоянии преступности в России за январь-февраль 2022 г. / Отчет Генпрокуратуры РФ / Портал правовой статистики. [Электрон. ресурс]. - URL: http://crimestat.ru/analytics (дата обращения: 10.04.2022).

5. Север Н.С. Некоторые особенности личности киберпреступников: криминологический аспект // Молодой ученый. - 2021. - № 53 (395). - С. 120-122.

6. Малби С., Мейс Р., Холтерхоф А., Браун К., Кашерус С., Игнатущенко Е. Всестороннее исследование проблемы киберпреступности / Доклад УНП ООН, 2013. - Австрия: Вена. - 360 с.

7. Пучков О.А. Социально-криминологический портрет хакера: концептуальный образ // Вопросы российского и международного права. - 2020. - № 3А. - Т. 10. - С. 60-71.

8. Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий // Вестник Томского гос. ун-та. - 2017. - № 299. - С. 180-181.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ ТОВАРНОЙ ПОЛИТИКИ ПРЕДПРИЯТИЯ

Аитов Д.В., *студент;*
Шайхутдинова Ф.Н., *канд. хим. наук, доцент,*
Университет управления «ТИСБИ», г. Казань

Аннотация. В статье исследованы особенности формирования товарной стратегии организации, проанализированы основные задачи ассортиментной политики. Рассмотрены стратегии управления товарной номенклатурой в компании «Светхолл».

Ключевые слова: товарная стратегия, товарная политика, ассортиментная политика, ассортимент предприятия.

Для успешной реализации предпринимательской деятельности необходимо, чтобы реализуемый товар или услуга находили спрос на рынке и были направлены на удовлетворение спроса потенциальных клиентов. Поэтому важно постоянно поддерживать конкурентоспособность товара на рынке. Процесс осуществляется благодаря специальному направлению в менеджменте - товарной политике.

Товарная стратегия компании представляет собой комплекс мероприятий, направленных на решение таких задач, как: что производить или продавать, в каком виде и объемах продавать, а также кому предоставлять товар. То есть товарная политика направлена на то, чтобы предлагать рынку те товары и услуги, в которых востребованы клиенты [2].

Создание и внедрение грамотной товарной политики предприятия - это одно из базовых условий для успешного существования организации, так как именно товар выступает эффективным методом воздействия на рынок. При этом важно соблюдать оптимальное соотношение между удовлетворением потребностей клиентов и получением выгоды от реализации товаров и услуг.

Необходимость работы с ассортиментом для улучшения

экономического состояния организации повышается в условиях рыночной экономики. Усовершенствованные продукты и товары находят повышенный спрос среди покупателей, соответственно приносят прибыль, повышают конкурентоспособные характеристики предприятия на рынке. Грамотно сформированная товарная политика служит для предприятия указателем направления его деятельности, играет важную роль при принятии текущих решений [1].

На современном этапе потребности клиентов постоянно меняются, поэтому предпринимателям приходится подстраиваться под запросы потребителей.

Чтобы определить конкретные потребности покупателей, необходимо проводить подробный анализ и выявлять такие важные факторы, как регион проживания, семейное положение, социальный статус, средний ежемесячный доход, возрастная категория и пол.

На экономическое положение предприятий большое воздействие оказывает ситуация во всем мире. Введение санкций против России, повышение курса рубля и доллара приводят к тому, что предпринимателям приходится искать новых поставщиков, подстраиваться под повышение цен на сырье и товары, при этом они не должны забывать и про потребности клиентов, которые хотят видеть разнообразный ассортимент по доступным ценам.

Частично решить данную проблему помогает грамотно подобранная товарная стратегия, которая направлена на решение следующих задач [3]:

- удовлетворение потребностей и запросов целевой аудитории - это основной принцип маркетинга, который необходим для глубокой сегментации рынка и обеспечения лояльности клиентов по отношению к компании;
- грамотное применение знаний и опыта организации при принятии управленческих решений;
- оптимизация финансовых показателей компании;
- создание ассортимента на основе ожидаемых показателей величины прибыли и рентабельности товаров;
- поиск новых клиентов, удлинение жизненного цикла товаров путем поиска новых рынков сбыта;
- применение принципа гибкости за счет расширения ассортимента и переориентации товаров сбыта;
- соблюдение закона синергии, то есть разработка такого набора элементов, при котором потенциал предприятия будет раскрыт на максимум.

Основным принципом при формировании ассортимента является типология наименований - это распределение товаров по характеру потребления и срокам использования, то есть разделение товаров на