Научная статья
УДК 331.5
EDN VDISAG
DOI 10.17150/2411-6262.2022.13(2).39

О.А. Старостенко
Краснодарский университет Министерства внутренних дел Российской Федерации, г. Краснодар, Российская Федерация, olegstaros94@gmail.com

ТЕХНИЧЕСКИЕ МЕРЫ ПРОФИЛАКТИКИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

АННОТАЦИЯ. Хищения, совершаемые с использованием информационно-телекоммуникационных технологий, занимают лидирующую позицию в киберпреступном мире и являются ведущей проблемой развивающихся стран. Обеспечение эффективности предупредительной деятельности в рассматриваемой сфере представляет собой определенную проблему, решение которой зависит от системного подхода к разрешению организационных и правовых аспектов специального предупреждения данного вида преступлений. Специфика IT-хищений (краж и мошенничеств) требует корректировки устоявшихся методов осуществления специальной профилактики и формирования новых подходов к такой деятельности (технологизации процесса). В работе автором выделен комплекс основных перспективных технических мер предупреждения IT-хищений, направленных на разработку и внедрение единой системы мониторинга (интеллектуальный анализ данных и извлечение полезных данных из общих объемов данных); борьбу с анонимностью (рассмотрена возможность деанонимизации пользователей) и противодействию мошенническому спаму (рассмотрена возможность использования технологии «серых списков»; введение специализированного тарифного плана при использования электронной почты; разработки отечественного программного обеспечения, основанного на индивидуальных байесовских фильтрах, способных анализировать статистику встречаемости слов в текстах мошеннических сообщений). Определены основные направления практической реализации предлагаемых подходов. В заключении автор акцентирует внимание на том, что применение указанных технических мер профилактики позволит всей системе предупреждения киберпреступности быть целостной и логически завершенной.

КЛЮЧЕВЫЕ СЛОВА. IT-хищения, профилактика преступлений, специальное предупреждение, технические меры, киберпространство, анализ данных.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 5 апреля 2022 г.; дата принятия к печати 25 мая 2022 г.; дата онлайн-размещения 10 июня 2022 г.

Original article

O.A. Starostenko
Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, Russian Federation, olegstaros94@gmail.com

TECHNICAL MEASURES FOR PREVENTION OF THEFT COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

ABSTRACT. Theft committed with the use of information and telecommunication technologies has taken a lead in cybercrimes and is a major concern of developing countries. Provision of effective prevention activity in the sphere under study poses a serious problem. Its solution depends on a systematic approach to resolving organizational and legal aspects of social prevention of this type of theft. The specificity

of IT-theft (stealing and fraud) calls for correction of established methods of special prevention measures and building new approaches to such activity (technologisation of the process). The article allocates a set of major perspective technical measures for prevention of IT-theft aimed to develop and implement a single monitoring system (data mining and extraction of useful data from total data volumes); the fight against anonymity (the possibility of de-anonymization of users is considered). The study also highlights countering fraudulent spam (the possibility of using the technology of «gray lists», the introduction of a specialized tariff plan when using e-mail as well as the development of domestic software based on individual Bayesian filters capable of analyzing the statistics of the occurrence of words in the texts of fraudulent messages). The main directions of practical implementation of the proposed approaches are determined. In conclusion, the author emphasizes the fact that the application of these technical preventive measures will allow the entire cybercrime prevention system to be holistic and logically complete.

KEYWORDS. IT-theft, crime prevention, special prevention, technical measures, cyberspace, data analysis.

ARTICLE INFO. Received April 4, 2022; accepted May 25, 2022; available online June 10, 2022.

В настоящее время хищения, совершаемые с использованием информационно-телекоммуникационных технологий (IT-хищения), обладают высокой латентностью, что серьезно осложняет установление виновных лиц, способствует появлению новых преступлений и провоцирует дальнейший рост нарушения законности [1, с. 71–76].

Обеспечение эффективности предупредительной деятельности в рассматриваемой сфере представляет собой определенную проблему, решение которой зависит от системного подхода к разрешению организационных и правовых аспектов специального предупреждения данного вида преступлений.

В науке криминологии профилактика преступной деятельности выступает одной из четырех разновидностей предупреждающих преступность действий: профилактика, предотвращение преступлений, пресечение совершаемых преступлений, исправление осужденных. Так, в целях минимизации негативных последствий необходимо тщательно анализировать состояние преступности, концепции причин преступности, особенности личности преступника и его жертвы [2, с. 141–146].

Профилактику хищений, совершаемых с использованием информационно-телекоммуникационных технологий, начали осуществлять с первых дней зарождения киберпространства, резкого скачка вперед науки и техники, диверсификации основных и создания новых беспроводных портативных устройств удаленного доступа.

Традиционно ее принято разделять в зависимости от характера и масштаба принимаемых мер на общесоциальную и специальную.

Общесоциальные меры профилактики, как правило, связаны с улучшением материального благосостояния граждан, условий их труда и отдыха, укреплением дисциплины и организованности, а также с другими позитивными изменениями в обществе. Это, прежде всего, изменения в социальной, политической, экономической, нравственной и правовой сферах [3, с. 120–128].

В целях борьбы непосредственно с преступлением необходимо воздействовать на причины и условия, обусловливающие его совершение, то есть действовать в рамках специальной профилактики.

По мнению Г.А. Аванесова, под специальной профилактикой необходимо понимать деятельность государственных, общественных и др. органов, призванных принимать меры к устранению причин и условий, способствующих совершению преступления [4, с. 331–342].

А.И. Долгова считает, что специальная профилактика имеет целенаправленный на недопущение преступлений характер. Ее профилирующий признак — специальная предназначенность для выявления и устранения причин, условий, иных детерминант преступности. Кроме того, специальная профилактика включает в себя предотвращение подготавливаемых и пресечение начатых преступлений [5, с. 34].

Г.Г. Шиханцов обращает внимание на целенаправленность и локализованность во времени и пространстве специальных профилактических мер. Также ученый полагает, что меры специальной профилактики принимаются в разрезе отдельных ее составляющих и временные ограничения [6, с. 42–57].

Согласно Федеральный закону от 23.06.2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», субъектами профилактики выступают: федеральные органы исполнительной власти, органы прокуратуры Российской Федерации, следственные органы Следственного комитета Российской Федерации, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также граждане, общественные объединения и иные организации, оказывающие помощь (содействие) субъектам профилактики правонарушений в рамках реализации своих прав в сфере профилактики правонарушений[1].

Необходимо отметить, что специфика хищений, совершаемых с использованием информационно-телекоммуникационных технологий, требует корректировки устоявшихся методов осуществления специальной профилактики и формирования новых подходов к такой деятельности.

Меры специальной профилактики хищений, совершаемых с использованием информационно-телекоммуникационных технологий целесообразно разделить на:

1. Технические;
2. Организационно-правовые;
3. Меры воздействия на население;
4. Индивидуальная работа с жертвой и преступником.

В рамках данной статьи остановимся на исследовании комплекса технических мер специальной профилактики.

Арсенал технических мер должен включать меры, реализуемые путем установки новых или модернизации используемых технических средств защиты информации. К таковым могли бы относиться:

1. *Разработка и внедрение единой системы мониторинга в целях предупреждения IT-хищений.*

Многие страны уже приняли проекты создания такой системы. Так, правительственные управления США, Индии, Великобритании предоставили за 2019 г. отчеты с подробным описанием деятельности по созданию интегрированной системы мониторинга в целях предупреждения сетевых мошеннических действий или краж (около 200 проектов в каждой из стран). Система способна производить интеллектуальный анализ данных и вычислительную разведку, сканировать сеть на предмет преступных действий, фиксировать нерегулярность и неправомерное поведение пользователей в сети Интернет (например, неоднократные попытки ввода пароля учетной страницы пользователя) [7, с. 17–41].

Реализация процесса разработки и внедрения системы мониторинга данных в повседневную деятельность в России должна быть подкреплена глубокими научными познаниями как о прикладной области, так и о методологии совершения информационно-телекоммуникационных хищений. Система на автоматическом

[1] Об основах системы профилактики правонарушений в Российской Федерации : Федер. закон от 23 июня 2016 г. N 182-ФЗ // СПС «КонсультантПлюс».

уровне должна производить интеллектуальный анализ веб-данных в целях противодействия исследуемому явлению.

В последнее десятилетие организация сбора данных является ведущей государственной задачей. Во многом это связано с виртуализацией деятельности, благодаря выдающимся достижениям, обусловленным появлением современной техники (персональные компьютеры, смартфоны, планшеты, смарт-браслеты и др. гаджеты). Тем не менее, необработанные данные необходимо постепенно преобразовывать в информацию, а впоследствии, в знания.

В 1989 г. Григорий Пятецкий-Шапиро (основатель и председатель SIGKDD — группы особых интересов, посвященной «открытию знаний в данных») разработал технологию, известную как обнаружение противоправных алгоритмов (путем поиска полезных знаний) в базах данных «Knowledge Discovery in Databases» (KDD) — извлечение полезных знаний из общих объемов данных и интеллектуальный анализ данных «Data Mining» (DM) — обнаружение знаний в базах данных, который представляет собой процесс применения вычислительных средств для обнаружения алгоритмов с использованием необработанных данных, выполняющий следующие функции: сбор и подготовка данных, поиск информативных признаков, фильтрации данных, использование методов DM, обобщение результатов.

Интеллектуальный анализ данных (DM) способен извлекать полезные и релевантные знания из больших гетерогенных, удаленных и разрозненных мультимедийных наборов, включающих, в частности, тексты, фотографии, видео, аудиосообщения. DM основан на компьютерных алгоритмах классификации, анализе ассоциативных связей, регрессии, кластеризации и, как правило, должен состоять из следующих этапов:

1. Создание первичного набора данных (посредством использования доступного спектра источников, происходит создание первичного набора данных).

2. Начальный этап обработки данных. Отбор криминологически значимой информации:

– выявление пользователей, потребляющих большой объем интернет-трафика;

– определение веб-сайтов с большим количеством рекламного программного обеспечения;

– поиск пользователей, занимающихся продажей товаров в Интернете по цене ниже рыночной;

– установление персональной информации о жертвах мошеннических действий в социальных сетях и на бесплатных сайтах частных объявлений о продаже;

– поиск заблокированных учетных записей;

– обнаружение скоростных финансовых потоков и вредоносных расширений и т.д.[2];

3. Трансформация данных. Приведение информации, с использованием квантования, к пригодному для анализа виду. Так, например, сегментация данных о жертвах Интернет-магазинов по возрасту, полу, социальному положению; о пользователях социальной сетью по публикационной активности, распространению медиа-текста (включая аудиовизуальный контент), количеству принадлежащих профилей. Также на данном этапе происходит отслеживание веб-страниц, на которых чаще всего пользователи прерывают просмотр сайта[3].

4. Непосредственно интеллектуальный анализ. Применение совокупности алгоритмов с целью нахождения «сырых» знаний. На данном этапе производится определение данных, значительно отличающихся от нормы, а также синергетический анализ взаимодействий лица с информационными телекоммуникациями

[2] SAS Institute. URL: http://sas.com (дата обращения: 21.03.2021).
[3] GartnerGroup. URL: http://gartner.com (дата обращения: 21.03.2021).

с целью автоматической идентификации преступников и обеспечения надежной защиты пользователей [8, с. 50–98].

5. Постобработка информации. Обобщение и отражение результатов в веб-приложениях, доведение до пользователей [9, с. 32–41].

Полагаем, что Методы DM-анализа должны использоваться правоохранительными органами с целью выявления подозрительных субъектов, способных совершать сетевые преступления, а также предоставлять информацию для обнаружения кибервторжений, извлекая полезные данные, выражающиеся в форме знаний, сохраняя при этом конфиденциальность и персональность.

Несмотря на то, что DM-анализ имеет много областей применения (промышленные условия, бизнес), наш дискурс ограничивается борьбой с IT-хищениями, которая включает в себя кибербезопасность (наблюдение за подозрительной деятельностью, личный мониторинг подозрительных групп посредством использования Интернета или мобильной связи). При производстве DM-анализа в целях специальной профилактики IT-хищений необходимо использовать интеллектуальные инструменты, выступающие важнейшими ресурсами, преобразующими имеющийся объем данных в полезные знания.

Необходимо отметить, что для успешного функционирования DM необходим высококвалифицированный персонал (эксперты, специалисты-аналитики), который способен производить анализ и получать необходимый результат. Автоматические данные, извлеченные в ходе использования интеллектуального анализа, должны быть изучены и проанализированы на выходе «вручную» пользователем. Достоверность полученных результатов зависит, от того, насколько они соответствуют принятой системой «нормальной картине» [10, с. 3]. Например, чтобы оценить силу приложения DM, предназначенного для выявления потенциальных угроз IT-хищений, пользователю должна предоставляться возможность протестировать модель, используя данные о зафиксированных случаях с целью идентификации подозреваемого, поведение которого будет значительно отклоняться от исходной модели.

Еще одно ограничение при осуществлении DM-анализа связано с тем, что он не способен распознать и обнаружить причинно-следственные связи. Например, приложение может классифицировать модель поведения (склонность покупать в Интернете авиабилеты незадолго до отправления рейса), в связи с такими характеристиками, как доход, уровень образования и использование Интернета, однако это не указывает на автоматику явления (что поведение при покупке билета вызвано одной или несколькими переменными). На поведение человека могут влиять и другие переменные, такие как профессия (необходимость совершать регулярные поездки в короткие промежутки времени), семейные обстоятельства (больной родственник, нуждающийся во внимании) или хобби (использование преимуществ сниженного тарифа для посещения новых пунктов назначения).

Резюмируя вышеизложенное, считаем, что разработанная интегрированная система мониторинга, в основе которой лежит анализ действий жертвы и злоумышленника, обеспечит сбор, оценку и возможность предупреждения хищений, совершаемых с использованием информационно-телекоммуникационных технологий, до момента их наступления. Управление системой, посредством использования распределенной вычислительной среды, включая механизмы управления атрибутами, токенизацию идентифицируемых данных, взвешивание рисков, нормализацию журналов и корреляцию данных позволит обеспечить процесс прогнозирования вероятности наряду с высоким уровнем достоверности.

2. *Противодействие анонимности.*

Все сети массовых коммуникаций — от телефонных сетей, используемых для голосовых телефонных звонков, до Интернета — нуждаются в централизованном

управлении и в разработке новых технических стандартов, способных обеспечить их безопасное функционирование.

Одной из проблем, связанной с отсутствием механизма контроля в глобальной сети, выступает способность пользователя анонимизировать и зашифровывать личные данные. Например, если провайдер блокирует доступ к веб-сайту, который содержит неправомерную информацию, пользователь, как правило, не может больше осуществить на него вход. Однако, используя анонимный коммуникационный сервер, шифрующий связь между ним и центральным сервером, злоумышленник избегает блокирования информации.

С целью противодействия анонимности М. Приходовский («Новая концепция развития Интернета в контексте задачи обеспечения информационной безопасности») предлагает персонифицировать подключения к информационно-телекоммуникационной сети Интернет при запуске веб-браузеров. Ученый считает, что компания-провайдер должна выдавать пользователям информационно-телекоммуникационными технологиями индивидуальные устройства USB и PIN-коды к ним. Принцип действия подобен SIM-карте и основывается на идентификации пользователя по персональному номеру карты, договор на которую составляется в офисах компьютерных компаний, что позволит предупреждать IT-хищения на начальных стадиях.

На этот счет А.А. Комаров отмечает, что идея внедрения электронного паспорта имеет перспективное будущее, но на сегодняшний день существует несколько недостатков, требующих корректировки, а именно: не определены реестродержатели электронных паспортов, удостоверяющих центров и владельцы всемирной базы персональных данных; слабая привязка Интернет-паспорта к личности, способная спровоцировать его подмену.

С целью устранения указанных недостатков им предложены следующие технические решения:

– неразрывная связь электронного паспорта с личностью пользователя. Для предотвращения несанкционированного использования паспорта, необходимо внедрение биометрических технологий идентификации личности;

– универсальность Интернет-паспорта. Автор предлагает объединить в себе платежное средство — пластиковую банковскую карту, технологию электронной цифровой подписи, позволяющей одновременно удостоверять документы и т.д. [11, с. 158–165]

Однако нами обнаружено, что идентификация пользователей в сети Интернет существует с момента ее основания — на уровне Интернет-провайдеров, когда по запросу уполномоченных органов (правоохранительных) предоставляется имеющаяся информация о пользователе IT-услугами, при которой становится возможным определить его привычки, место жительства, трудоустройство, а зачастую и личность. Другими словами, анонимности в сети Интернет, как таковой, не существует (существует подмена IP, шифрование). Полагаем, что киберпреступники, подобно преступникам физического мира, свою область преступной деятельности познали в полной мере (умеют скрывать информацию о себе; знают, как устроен Интернет). Как правило, и те и другие имеют несколько паспортов, что в данном случае подтверждает неэффективность паспортизации.

Раскрывая мысль далее, задумаемся о возможных последствиях персонификации (что произойдет, если все пользователи информационно-телекоммуникационными технологиями будут обладать идентификационным номером?). Скорее всего, преступники зарегистрируют на свое имя две учетные записи, каждой из которых будет присущ индивидуальный идентификационный номер, как это происходит в реальной жизни с поддельными паспортами и номерами. Данное действие позволит им вновь успешно осуществлять свой умысел «анонимно».

Порядочный же идентифицированный пользователь IT-услугами в такой ситуации будет определяться как реальная личность, распознать которую не составит труда не только уполномоченным органам, но и преступникам. Следовательно, совершаемые онлайн-операции с денежными средствами на банковском счете, посредством использования системы «мгновенных» платежей, сделают таких пользователей объектом наблюдения заинтересованных лиц. Кроме того, предложенная техническая мера противоречит ч. 1 ст. 9 действующего ФЗ от 27.07.2006 г. № 152-ФЗ (ред. от 30.12.2020 г.) «О персональных данных» (с изм. и доп., вступ. в силу с 01.03.2021 г.), согласно которой субъект персональных данных принимает решение о предоставлении данных и дает согласие на их обработку свободно, своей волей и в своем интересе. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных, полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором[4]. В этой связи возникает вывод, что сбор персональных данных без добровольного согласия пользователей сделает их потенциально уязвимыми и беззащитными.

Рассматривая проблему лишения пользователей анонимности с другой стороны, остановимся на примере отдельно взятой страны. Многим известен тот факт, что информационно-телекоммуникационная сеть, в частности Интернет, имеет свои доменные зоны (границы). Каждая страна, как правило, характеризуется своими границами. Допуская возможность ввода системы электронных паспортов в России, зададимся вопросом идентификации зарубежных пользователей отечественными веб-сайтами. В данном случае правительства иностранных государств обязаны выдавать всем своим Интернет-пользователям паспорта, которые принимались бы в нашей стране. Однако такая идея не является приемлемой, так как во многих странах виртуальная мошенническая деятельность является одной из основных статей дохода [12, с. 716–725]. Ввиду этого, электронную паспортизацию все же придется вводить в рамках одной страны. Такие действия, вероятностно, отграничат российских пользователей от всего свободного мирового Интернета и сузят круг деловых интересов. Решить проблему представляется возможным на уровне международного сотрудничества, однако ни одного успешного примера в истории человечества, когда все страны мира смогли договориться о чем-либо, зафиксировано до сих пор не было. Таким образом, деанонимизация может привести к таким процессам, как:

– повышение виктимности рядовых пользователей Интернет-услугами;
– преобразование страны в тоталитарное государство;
– порождение новых мошеннических рисков;
– изоляция отечественного киберпространства;
– увеличение риска мошеннических действий с персональными данными;
– необоснованный рост государственных расходов наряду с уменьшением уровня технической защищенности пользователей.

Вследствие этого, предлагаем от проблемы противодействия сетевой анонимности перейти к проблеме технической защищенности пользователей в киберпространстве от мошеннического спама.

3. *Противодействие мошенническому спаму.*

У начинающих пользователей информационно-телекоммуникационными технологиями «спам» обычно ассоциируется с письмами рекламного характера, однако это не совсем так: спам некоторых видов преследует совсем иные цели. Одна из самых опасных разновидностей спама — мошеннические письма («онлайн-бла-

[4] О персональных данных : Федер. закон от 27 июля 2006 г. № 152-ФЗ : (ред. от 30 дек. 2020) // СПС « КонсультантПлюс».

готворительность», «Нигерийские письма», фиктивные уведомления о выигрыше в лотерею, «ошибки» платежных систем, «фиктивные казино», дистанционное трудоустройство и т.д.). Мошеннические «спамовые» письма рассылаются пользователям с целью распространения заведомо ложных сведений и хищения их денежных средств.

К концу 2020 г. практически все Интернет-провайдеры ввели запрет на рассылку спам-сообщений[5]. Однако, несмотря на наличие большего количества современных антиспам-фильтров, нацеленных на защиту хостов, выявление спама и принятие необходимых упреждающих мер, сумма ущерба от мошеннических писем и краж с каждым годом лишь увеличивается[6]. Это свидетельствует о низкой эффективности данного программного обеспечения.

Технические средства борьбы со спамом, широко применяемые в настоящее время, в большей мере основаны на фильтрации по содержимому сообщения в комбинации с использованием черных списков. Основным побочным эффектом такого действия выступает ложное распознание сообщений, в результате которого пользователь, в силу своей доверчивости или случайным образом, может осуществить переход по мошеннической веб-ссылке и вступить в диалог со злоумышленником. В свою очередь провайдер, проводя периодическую фильтрацию спама на всех почтовых ящиках зачастую уничтожает все «спамовые» письма, а не копирует их в специальную папку (в отдельных случаях такие письма могут оказаться желательными, например, ввиду неверного распознания или с целью их использования, как материала для исследований).

В качестве создания нового подхода к предупреждению сетевого спама М. Рамендик предложил использовать средства защиты, которые проверяют отправителя каждого почтового письма на подлинность (всегда, либо в случае, если ранее с данного электронного адреса сообщения не приходило). В ответ на письмо отправляется запрос, на который отправителю необходимо отвечать вручную, например, прочесть запись на полученной картинке, перепечатать и отправить ее ответным письмом[7]. Такие действия позволят отличить реального пользователя от роботизированной системы. К сожалению, данный подход был раскритикован, так как противоречил главному преимуществу электронной почты — возможности мгновенной доставки писем. До того, как отправитель получит извещение и пройдет проверку, его письмо не будет доставлено адресату. Кроме того, подобные системы неадекватно работают со списками рассылки, на которые подписан пользователь. Получение письма из списка рассылки может привести к тому, что запрос на подтверждение подлинности будет направлен в адрес всех ее участников.

Следующей относительно новой мерой является технология создания «серых списков[8]». Принцип работы основан на составлении списка серверов, от которых пользователь принимает почту и анализ их поведения. Алгоритм действия почтового сервера и данной программы существенно различается, однако преступники уже начали приспосабливать свои программные обеспечения к его действию.

Одной из устоявшихся технологий противодействия спаму выступает контентная фильтрация. Спам-письмо проверяется на наличие мошеннических фрагментов, картинок и др. характерных черт. Приложение способно производить интеллектуальный подсчет «спамерского веса» электронного письма [13, с. 124].

[5] Kaspersky / АО «Лаборатория Касперского». 2022. URL: https://www.kaspersky.ru/home-security?campaign=kl (дата обращения: 12.05.2021).

[6] Министерство Внутренних Дел РФ : офиц. сайт. М., 2022. URL: https://мвд.рф/vsmi/ Sodruzhestvo/item/23854147 (дата обращения: 12.05.2021).

[7] Библиотека nnre.ru. URL: http://www.nnre.ru/ (дата обращения: 12.05.2021).

[8] Библиотека NeroHelp. URL: http://nerohelp.info/15336-chto-takoe-serye-spiski.html (дата обращения: 12.05.2021).

Поскольку фильтр существует относительно давно, злоумышленники изобрели технологии обхода данной системы путем использования небуквенных символов и генерации цветных фонов.

По нашему мнению, результативной мерой предупреждения мошеннических рассылок могла бы стать — введение специализированного тарифа, исходя из которого, каждое доставленное электронное письмо должно быть оплачено. Стоимость сообщения определяется тарифом и начинается, например, от одного рубля. Полагаем, что при стандартном использовании электронной почты размер оплаты будет незаметным — но массовые распространения писем окажутся слишком дорогими. Необходимо понимать, что создание такой системы должно быть подкреплено созданием масштабной технической инфраструктуры и надежной системы «быстрых платежей, способных функционировать во всем мире.

Следующей действенной мерой профилактики IT-хищений может выступить разработка отечественного программного обеспечения, основанного на индивидуальных байесовских фильтрах, способных анализировать статистику встречаемости слов в текстах сообщений. Сущность Байесовских фильтров заключается в уникальном настраивании системы под тематики писем, типичных для мошенников, следовательно, внедрение их в рабочее приложение будет способствовать минимизации причиняемого ущерба [14, с. 32–34]. По этому поводу в 2018 г. размышляли специалисты Electronic Frontier Foundation. Они пришли к выводу, что программа способна обеспечить положительный результат, если пользователям электронных почтовых ящиков будет предоставлена возможность их приобретать без встроенной функции фильтрации спама, так как бесконтрольный поток спама более допустим, чем результаты работающих сегодня фильтров, а совместные действия нескольких приложений приводят к техническим сбоям и неверной идентификации писем [15, с. 1008–1027].

В 2019 г. в Лондоне состоялся запуск такого приложения: «Уже при обучении на 1 500 сообщений была достигнута точность классификации более 97 %. Думается, со временем она повысится до 99,9 %, что позволит практически полностью ликвидировать мошеннический спам». На сегодняшний день эффективность приложения оправдана, так как точность классификации составляет 98,3 % [16, с. 157–166].

Вполне возможно, что такое приложение в нашей стране появится не скоро и основные области его применения к тому времени изменятся. Однако существующие технологии фильтрации мошеннического спама достигли практически своего предела и требуют срочных инновационных решений. Полагаем, что для реализации данного метода, в первую очередь, Интернет-провайдерам необходимо наделить пользователей возможностью управлять встроенным фильтрами вручную с функцией их полного отключения. Во-вторых, все реализуемые современные средства обработки данных должны содержать разработанную и настроенную для работы такую программу по умолчанию.

Подводя итог, отметим, что существующие меры предупреждения хищений, совершаемых с использованием информационно-телекоммуникационных технологий малоэффективны. Об этом свидетельствует стремительный рост рассматриваемой категории преступлений. Считаем, что разработка и дальнейшее комплексное использование указанных нами технических мер позволит в будущем снизить количество преступлений рассматриваемого вида.

Список использованной литературы

1. Старостенко Н.И. Криминалистическое понимание механизма совершения мошенничества с использованием методов социальной инженерии / Н.И. Старостенко // Общество и право. — 2021. — № 1 (75). — С. 71–76.

2. Антонян Ю.М. Криминология : учебник / Ю.М. Антонян. — 3-е изд., перераб. и доп. — Москва : Юрайт, 2018. — 388 с.

3. Криминология : учебник / под ред. В.Д. Малкова. — 2-е изд., перераб. и доп. — Москва : Юстицинформ, 2006. — 528 с.

4. Криминология : учебник / под ред. Г.А. Аванесова. — 5-е изд., перераб. и доп. — Москва : Юнити-Дана, 2012. — 575 с.

5. Долгова А.И. Организованная преступность, ее развитие и борьба с ней / А.И. Долгова // Организованная преступность-3 / под ред. А.И. Долговой, С.В. Дьякова. — Москва, 1996. — С. 6–56.

6. Шиханцов Г.Г. Криминология : учеб. пособие / Г.Г. Шиханцов. — Минск : Тесей, 2006. — 296 с.

7. Jans M. Internal fraud risk reduction: Results of a data mining case study / M. Jans, N. Lybaert, K. Vanhoof // International Journal of Accounting Information Systems. — 2010. — Vol. 11, no. 1. — P. 17–41.

8. Методы и модели анализа данных: OLAP и Data Mining / А.А. Барсегян, М.С. Куприянов, В.В. Степаненко, И.И. Холод. — Санкт-Петербург : БХВ-Петербург, 2007. — 336 с.

9. Когнитивная бизнес-аналитика / под ред. Н.М. Абдикеева. — Москва : Инфра-М, 2011. — 510 с.

10. Bhowmik R. Data mining techniques in fraud detection / R. Bhowmik // Journal of Digital Forensics, Security and Law. — 2008. — Vol. 3, no. 2. — P. 35–54.

11. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет : дис. … канд. юрид. наук : 12.00.08 / А.А. Комаров. —Пятигорск, 2011. — 262 с.

12. Adomi E.E. Combating cyber crime in Nigeria / E.E. Adomi, S.E. Igun // The Electronic Library. — 2008. — Vol. 26, no. 5. — P. 716–725.

13. Ларионова А.В. Метод фильтрации спама на основе искусственной нейронной сети / А.В. Ларионова, П.Б. Хорев // Науковедение. — 2016. — Т. 8, № 3 (34). — URL: https://elibrary.ru/download/elibrary_26535175_29420754.pdf.

14. Семенова М.А. Метод автоматической фильтрации при борьбе со «спамом» / М.А. Семенова, В.А. Семенов // Известия высших учебных заведений. Приборостроение. — 2009. — Т. 52, № 9. — С. 32–34.

15. Postigo H. Capturing fair use for the YouTube generation: The digital rights movement, the Electronic Frontier Foundation and the user-centered framing of fair use / H. Postigo // Information, communication & society. — 2008. — Vol. 11, no. 7. — P. 1008–1027.

16. Caverlee J. Countering web spam with credibility-based link analysis / J. Caverlee, L. Liu // Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing. — 2007. — P. 157–166.

References

1. Starostenko N.I. Criminalistic understanding of the mechanism of committing fraud using social engineering methods. Obshchestvo i pravo = Society and Law, 2021, no. 1, pp. 71–76. (In Russian).

2. Antonyan Yu.M. Criminology. Moscow, Yurait Publ., 2018. 388 p.

3. Malkov V. D. (ed.). Criminology. 3rd ed. Moscow, Yustitsinform Publ., 2006. 528 p.

4. Avanesov G.A. (ed.). Criminology. 5th ed., Moscow, Yuniti-Dana Publ., 2012. 575 p.

5. Dolgova A.I. Organized Crime, its Development and the Fight against it. In Dolgova A.I., D'yakov S.V. (eds). Organized crime-3. Moscow, 1996, pp. 6–56. (In Russian).

6. Shikhantsov G.G. Criminology. Minsk, Tesei Publ., 2006. 296 p.

7. Jans M., Lybaert N., Vanhoof K. Internal fraud risk reduction: Results of a data mining case study. International Journal of Accounting Information Systems, 2010, vol. 11, no. 1, pp. 17–41.

8. Barsegyan A.A., Kupriyanov M.S., Stepanenko V.V., Kholod I.I. Methods and models of data analysis: OLAP and Data Mining. Saint-Petersburg, BKhV-Peterburg Publ., 2007. 336 p.

9. Abdikeev N.M. (ed.). Cognitive business intelligence. Moscow, Infra-M Publ., 2011. 510 p.

10. Bhowmik R. Data mining techniques in fraud detection. Journal of Digital Forensics, Security and Law, 2008, vol. 3, no. 2, pp. 35–54.

11. Komarov A.A. Criminological aspects of fraud in the Internet global network. Cand. Diss. Pyatigorsk, 2011. 262 p.

12. Adomi E.E., Igun S.E. Combating cyber crime in Nigeria. The Electronic Library, 2008, vol. 26, no. 5, pp. 716–725.

13. Larionova A.V., Khorev P.B. Spam filtering method based on artificial neural network. Naukovedenie = Science Studies, 2016, vol. 8, no. 3. Available at: https://elibrary.ru/download/elibrary_26535175_29420754.pdf. (In Russian).

14. Semenova M.A., Semenov V.A. Automated filtration method for spam control. Izvestiya vysshikh uchebnykh zavedenii. Priborostroenie = Journal of instrument engineering, 2009, vol. 52, no. 9, pp. 32–34. (In Russian).

15. Postigo H. Capturing fair use for the YouTube generation: The digital rights movement, the Electronic Frontier Foundation and the user-centered framing of fair use. Information, communication & society, 2008, Vol. 11, no. 7, pp. 1008–1027.

16. Caverlee J., Liu L. Countering web spam with credibility-based link analysis. Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing, 2007, pp. 157–166.

Информация об авторе

Старостенко Олег Александрович — адъюнкт, кафедра уголовного права и криминологии, Краснодарский университет Министерства внутренних дел Российской Федерации, г. Краснодар, Российская Федерация, olegstaros94@gmail.com, https://orcid.org/0000-0002-8031-6915, SPIN-код: 7272-0275, AuthorID РИНЦ: 1060102.

Author

Oleg A. Starostenko — PhD Student, Department of Criminal Law and Criminology, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, Russian Federation, olegstaros94@gmail.com, https://orcid.org/0000-0002-8031-6915, SPIN-Code: 7272-0275, AuthorID RSCI: 1060102.

Для цитирования

Старостенко О.А. Технические меры профилактики хищений, совершаемых с использованием информационно-телекоммуникационных технологий / О.А. Старостенко. — DOI 10.17150/2411-6262.2022.13(2).39. — EDN VDISAG // Baikal Research Journal. — 2022. — Т. 13, № 2.

For Citation

Starostenko O.A. Technical Measures for Prevention of Theft Committed with the Use of Information and Telecommunication Technologies. *Baikal Research Journal*, 2022, vol. 13, no. 2. (In Russian). EDN: VDISAG. DOI: 10.17150/2411-6262.2022.13(2).39.