6. Сидоренко Л. И. Новые криминологические параметры измерения коррупции в России // Вестник Московского университета МВД России. 2017. № 4. С. 121–125.
7. Федотова Е. Н. Понятие и современное состояние взяточничества // IV Международный пенитенциарный форум «Преступление, наказание, исправление» Сборник тезисов выступлений и докладов участников. Рязань. 2019. С. 280–281.
8. Щербович И. А., Караев Р. Ш. Анализ детерминантов низовой коррупционной преступности в России // Правовая политика и правовая жизнь. 2017. № 2. С. 69–76.

УДК 343.98

ОТДЕЛЬНЫЕ ИНСТРУМЕНТЫ ПРОТИВОДЕЙСТВИЯ ЦИФРОВЫМ АТАКАМ

А. Р. Лонщакова, *кандидат юридических наук, доцент, доцент кафедры оперативно-разыскной деятельности органов внутренних дел Уфимского юридического института МВД России*

Статья посвящена особенностям противодействия фишингу и другим цифровым атакам. Своевременное выявление признаков фишинга, других цифровых атак и грамотное, комплексное реагирование на них позволит более эффективно предупреждать эти явления в цифровой сфере.

Ключевые слова: цифровая атака, признаки, выявление, принципы реагирования на цифровые атаки, алгоритм действий, нейтрализация, документирование, предупреждение, ответственность

INDIVIDUAL COUNTERACTION TOOLS DIGITAL ATTACKS

A. R. Lonshchakova, *Candidate of Law, Associate Professor, Associate Professor of the Department of Operational Investigative Activities of Internal Affairs Bodies of the Ufa Law Institute of the Ministry of Internal Affairs of Russia*

This article is devoted to the peculiarities of countering phishing and other digital attacks. Timely detection of signs of phishing and other digital attacks and a competent, comprehensive response to them will allow us to more effectively prevent these phenomena in the digital sphere.

Keywords: digital attack, signs, detection, principles of responding to digital attacks, algorithm of actions, neutralization, documentation, prevention, responsibility

Противодействие фишингу и другим цифровым атакам в сфере информационных технологий требует концептуально нового подхода: в первую очередь необходимо консолидировать ресурс в теоретической, организационно-тактической, методической направлениях.

В современных условиях для обеспечения информационной безопасности необходимо создание единой и комплексной инфрастуктуры для защиты всего киберпространства. Злоумышленники пытаются преодолеть, нейтрализовать систему защиты и получить доступ к охраняемой информационной среде, используя для этих целей современные технические возможности и социальную инженерию.

Кибербезопасность с точки зрения методологии основывается на трех базовых составляющих:

– технологического продукта (например, программные средства, средства защиты);

– персонала, который занимается обслуживаем информационных технологий в области информационной безопасности;

– процессов и явлений в области информационной безопасности (именно процессы и явления являются связующим звеном между технологическим продуктом и персоналом).

Знание закономерностей процессов и явлений в области информационной безопасности позволяет спрогнозировать подготовку, совершение атак, выявить, зафиксировать следовую картину, выявляя при этом уничтоженную, сфальсифицированную, замаскированную сокрытую следовую картину в целях построения криминалистической характеристики преступления, выдвижении общих и частных криминалистических версий, предупреждения цифровых атак.

Основная проблема на сегодняшний момент – это не технические атаки и вредоносное программное обеспечение: понятно, как с этим бороться. Есть технические методы и методы через изменение законодательства. Самая большая проблема – это социальная инженерия (фишинг, троянский конь, кви про кво, дорожное яблоко, обратная социальная инженерия, сбор из открытых источников и др.).

Анализ теории и практики выявления и противодействия цифровым атакам показал, что предпринимаемые меры по их предупреждению носят блочный характер, направлены на нейтрализацию отдельных угроз.

В этой связи, мы полагаем, что эффективное противодействие цифровым атакам базируется на четырех основных системных алгоритмах:

I. Алгоритма анализа исследования закономерностей (характеристик) цифровых атак – важно выявить их информативные особенности (маркеры), в том числе психологию поведения злоумышленника, его уязвимости.

II. Алгоритма реагирования на цифровые атаки – необходимо обучение предупреждению, распознаванию атак пользователей, их фиксации (сохранении цифровых следов).

III. Алгоритма оперативного взаимодействия пользователей при выявлении цифровых атак с правоохранительными органами.

IV. Алгоритма оперативного взаимодействия правоохранительных органов (в том числе международных, межведомственных, внутриведомственных) с кредитными организациями, операторами сотовой связи, специалистами и др.

Далее раскроем отдельные их особенности.

I. I. По результатам исследования закономерностей фишинга и других цифровых атак, выявлены отдельные значимые информативные их особенности (характеристики), анализ и использование которых позволит их нейтрализовать:

I. Личность злоумышленника характеризуется:

а) двумя группами лиц: находящихся в местах исполнения наказания за отдельные виды хищений, в том числе специализирующихся на цифровом мошенничестве, и всех остальных;

б) базовыми акцентуациями характера: гипертимной, демонстративной (истероидной), эпилептоидной. Акцентуации характера злоумышленников образуют алгоритмизированный стереотип психологии их поведения при подготовке и совершения цифровых атак, выбор методов противодействия выявлению криминалистически значимой информации.

I.II. Личность потерпевшего характеризуется отсутствием у них информации о личности злоумышленника, о его психологии поведения, способов совершения фишинга и других цифровых атак, способов сокрытия следовой картины цифровой атаки, методов их нейтрализации.

Социально-психологические характеристики пользователя (потерпевшего) отражают психологические черты, актуальные потребности, демографические характеристики, особенности когнитивных процессов, оценочное личностное отношение, способы поведения. Они же являются виктимологическими особенностями.

Личный опыт пользователя (например, особенности анализа объема исходящей информации, опыта столкновения с фишинг-атаками, знание основ информационной безопасности, умение распознавать индикаторы безопасности) влияет на возможность нейтрализации и предотвращения цифровых атак.

По результатам исследования, психологическими векторами атаки явились: любопытство, невнимательность, страх, жадность, желание помочь, раздражение. Важно отметить, что индуцируемые эмоции потерпевших в реализации цифровых атак явились и закономерностями психологии их поведения на манипулятивные техники злоумышленников.

I.III. Обстановка, условия фишинга и других цифровых атак характеризуются использованием сети Интернет (в социальных сетях, в интернет-магазинах, торговых интернет-ресурсах) и использованием средств мобильной телефонной связи, подключенных к сети Интернет (блокировка счета, банковской карты, незаконное списание денежных средств; маскировка хищений под видом социальных выплат, реализации социальных ресурсов и компенсаций).

Ссылки и фишинг-атаки осуществляются по электронной почте, со ссылками и мошенническими страницами, например, вредоносные вложения, атаки по электронной почте с вложенными файлами; в социальных сетях: атаки злоумышленников на пользователей; через мобильные устройства: атаки злоумышленников по телефону, на смартфоны и мобильных пользователей; с использованием технологий искусственного интеллекта; в реальной жизни: цифровые атаки в физическом мире, например, пользуясь моментом злоумышленники наносят цифровые атаки на тему COVID.

Модель антифишинга реализуется через обнаружение и восприятие цифровой атаки.

Внешний вид атаки характериуется визуальным оформлением, узнаваемым авторитетным брендом, аттрибуцией и персонификацией. Брендами, которыми прикрываются мошенники, являются известные российские банки, компании газовой, нефтяной отрасли, проекты Илона Маска – автомобильный Tesla и космический SpaceX. Мошеннические интернет-ресурсы представляют из себя страницу с красочным заголовком и ссылкой на видео с преимуществами проекта. В нижней части страницы – форма для сбора личных данных для последующего использования в рамках социальной инженерии.

I.IV. Типовыми способами противодействия злоумышленников выявлению значимой информации явились следующие: выход в сеть злоумышленником из зоны WI-FI, изменение «МАК –адреса», выход в сеть через подставные IP–адреса, уничтожение, фальсификация, утаивание следовой картины в информационной среде, в том числе с использованием программных продуктов, и др.

II. По результатам исследования, эффективными инструментами противодействия цифровым атакам явились следующие меры:

II.I. Обучение и тренировка навыков законопослушных граждан (пользователей) с отработкой следующих вопросов:

1) что они должны знать и уметь, какие навыки влияют на безопасность;

2) как пользователи открывают письма и переходят по ссылкам: открывают вложенные файлы, вводят данные в формы, подключают съемные устройства;

3) какие психологические и организационные векторы покрыты;

4) что должны знать об объективных метриках безопасности;

5) что делать при выявлении цифровых атак, алгоритм реагирования, особенности фиксации значимой информации;

6) как обучить пользователей выявлению и предупреждению цифровых атак.

В этой связи интересен пример Сбербанка России по обучению кибербезопасности своих клиентов. Так, например, клиенты Сбербанка России проходят курсы и сдают интерактивные тесты по вопросам безопасности; получают имитированные атаки по разным каналам и тренируют навыки: совершают или не совершают обучающиеся опасные действия, получают обратную связь. Статистика по обучению и тренировкам навыков поступает в антифрод-систему как дополнительные метрики поведения по каждому клиенту.

Дополнительными метриками для антифрода по каждому обучающемуся явились: уровень знаний, уровень навыков, опасные уязвимости программного обеспечения.

В этой связи, ФинЦЕРТ Сбербанка России рекомендует: повышать киберграмотность населения; доводить до клиентов информацию о необходимости неукоснительного соблюдения рекомендаций по выявлению и нейтрализации цифровых атак; повышать качество работы операторов в области осведомления своих клиентов в вопросах киберграмотности.

Специалисты по кибербезопасности рекомендуют тренировать и измерять эти навыки с подготовкой системного отчета и дополнительного обучения по следующей формуле: знания и навыки с возможностью их измерения, корректировки с постоянной их тренировкой (знаний, умений, навыков) [1, с. 10–14].

II.II. Для предупреждения фишинга и других цифровых атак специалисты в области IT-технологий и социальной инженерии рекомендуют усложнить злоумышленникам задачу [13, с. 163–165]:

1. Шифруйте, шифруйте и еще раз шифруйте–особенно всю конфиденциальную электронную корреспонденцию.

2. Используйте безопасный браузер.

3. Используйте безопасный IM-сервис с шифрованием.

4. Держите наготове вспомогательные VoIP-сервисы.

5. Используйте сервисы безопасного обмена сообщениями и переключайтесь между ними.

6. Используйте VPN (VPN – виртуальная частная сеть (Virtual private network).

7. Обновляйте программное обеспечение.

8. При общении по мобильному устройству с предполагаемым злоумышленником достаточно задать ряд уточняющих вопросов, чтобы понять от кого на самом деле поступил звонок: фамилию, имя, отчество, должность, номер рабочего кабинета, рабочий телефон, просьбу прислать официальный документ в установленном порядке с необходимыми реквизитами. Основное предостережение: не сообщать по телефону свои персональные данные.

Главное помнить о том, чтобы не случилось – ничего не случилось. При любых обстоятельствах необходимо сохранять спокойствие и готовность действовать хладнокровно.

Учитывая, что не все инциденты могут быть первоначально распознаны или обнаружены, должны существовать процедуры для определения неудачных и удачных попыток нарушения кибербезопасности. В зависимости от масштабов ущерба, причиняемого конкретным инцидентом, может возникнуть необходимость в консультации экспертов для определения корневой причины инцидента, оценки эффективности реагирования и в случае ущерба для сохранения цепочек свидетельств – для судебного преследования преступника [7, с. 338–339].

Понимание реагирования на фишинг и другие цифровые атаки, понимание влияния риска на безопасное функционирование информационной среды в случае появления угрозы в форме фишинга и других цифровых атак позволит предупреждать и нейтрализовать атаки в киберпространстве.

II.III. Ужесточение ответственности за противоправные посягательства в информационной сфере, нормативное правовое регулирование ответственности [12, с. 167–168].

III. Оперативное взаимодействие потерпевших с правоохранительными органами.

Детализированный опрос (допрос) потерпевших, изъятие и осмотр средств мобильной связи и компьютерной техники, проведение отдельных сыскных мероприятий: наведение справок (направление запроса в необходимые кредитные организации, операторам сотовой связи, в специальные технические подразделения); снятие информации с технических каналов связи; сбор образцов для сравнительного исследования, назначение и производство судебных экспертиз и иные мероприятия (оперативно-разыскные мероприятия и следственные (процессуальные) действия) позволят выявить и задокументировать криминалистически значимую информацию [2; 3; 4; 5; 6; 7, 8, 10, 11].

Основное внимание необходимо уделить, созданию условий для сохранения, фиксации, возможности ее использования при принятии юридически важных процессуальных и криминалистических решений [7, с. 338–339].

Важно отметить, что никакие технические средства защиты не помогут, если человек не будет самостоятельно осознавать серьезность кибератак, свое место и роль в их выявлении, противодействии им.

В завершении необходимо отметить, что при выявлении фишинга и других цифровых атак необходимо действовать и реагировать оперативно, выявляя максимальное количество значимой информации. Важно разобраться в ситуации, держать ее под контролем и готовиться к худшему [9, с. 87–99].

Проанализированные положения целесообразно сформулировать в виде принципов реагирования на фишинг и другие цифровые атаки в целях максимального и эффективного выявления и фиксации криминалистически значимой информации. Немалые перспективы принципы реагирования на фишинг и другие цифровые атаки способны открыть для правоохранительных органов. Сегодня

назрела необходимость в интеграции и кооперации информационно-технологических, юридических, финансовых систем для успешного взаимодействия и сотрудничества в области обеспечения кибербезопасности личности.

Список источников

1. Антонов В. В., Калимуллин Н. Р., Харисова З. И., Герфанова М. Р. Проблемы правового регулирования сферы искусственного интеллекта. В сборнике: Информационные технологии интеллектуальной поддержки принятия решений (ITTDS'2020). Труды VIII Всероссийской научной конференции (с приглашением зарубежных ученых). В 2-х томах. Уфа, 2020. С. 10–14.
2. Гаврилин Ю. В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: дис. … докт. юрид. наук, М., 2009. 404 с.
3. Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С. 45–50.
4. Гаспарян Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: дис. … канд. юрид. наук, М., 2020. 300 с.
5. Грибунов О. П. Средства сотовой связи как источник криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2017. № 4 (83). С. 137–142.
6. Лавров В. П. Противодействие расследованию преступлений и меры по его преодолению: учебник. Москва: Академия Управления МВД России, 2017. 147 с.
7. Лонщакова А. Р. Возможность выявления криминалистически значимой информации при анализе реагирования на киберинциденты // Евразийский юридический журнал. 2021. № 2. С. 338–339.
8. Мазуров И. Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. … канд. юрид. наук. Казань, 2017. 188 с.
9. Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // LexRussica. 2019. № 3 (148). С. 87–99.
10. Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … канд. юрид. наук. М., 2016. 249 с.
11. Шмонин А. В., Баранов В. В. Организация выявления, раскрытия и расследования хищений денежных средств в системе дистанционного банковского обслуживания: учебно-практическое пособие / под. ред. А. В. Шмонина. М.: Академия управления МВД России, 2014. 310 с.
12. Харисова З. И., Лонщакова А. Р. Обеспечение прав и свобод гражданина в области использования цифровых финансовых активов // Евразийский юридический журнал. 2020. № 3 (142). С. 167–168.
13. Харисова З. И., Файзулова Р. Р., Дюсьмекеева Д. С. Современные угрозы информационной безопасности в условиях глобализации информационного пространства. В сборнике: Актуальные проблемы кибербезопасности в сети Интернет. Сборник научных трудов Всероссийской конференции. 2020. С. 163–165.