УДК 004.056

Исследование технологий социоинженерных атак на пользователей сетевых ресурсов кредитно-финансовых организаций

Выполнено исследование технологий проведения социоинженерных (социотехнических) атак на пользователей сервисов дистанционного банковского обслуживания (ДБО) кредитно-финансовых организаций (КФО). Описана базовая структура проведения таких атак. Предложены подходы по противодействию алгоритмам/подходам, используемым киберпреступниками.

В.В. МАЛИКОВ,
к. т. н., доцент, начальник цикла технических и специальных дисциплин

Центр повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь

А.В. МАКАТЕРЧИК,
аспирант кафедры «Защита информации» УО «Белорусский государственный университет информатики и радиоэлектроники»

Ключевые слова:
ДБО, КФО, социоинженерная (социотехническая) атака, вредоносное программное обеспечение.

Введение. В настоящее время в мире и Республике Беларусь значительно возрастает число инцидентов, связанных с несанкционированным доступом (НСД) к сетевым ресурсам КФО.

По данным компании Positive Technologies, главным мотивом злоумышленников при совершении кибератак является получение финансовой выгоды (65 % инцидентов в 2018 году и 92 % в 2017 году) [1]. Системы безопасности кредитно-финансовых организаций, как правило, имеют высокий уровень ИБ, поэтому одним из главных векторов проникновения в каналы ДБО КФО являются методы социальной инженерии: 49 % от общего числа атак за 2018 год (рис. 1).

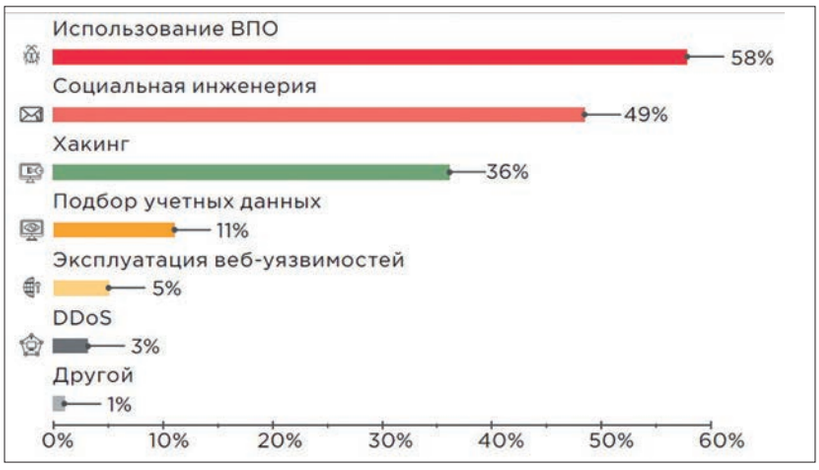


Рисунок 1 – Методы атак на КФО (за 2018 год) [1]

В рамках настоящей статьи предлагается авторская формулировка термина «социальная инженерия» (СИ) – совокупность приемов, методов и технологий, основанных на социальном и психологическом вредоносном воздействии (манипуляции) на сознание человека (пользователя), результатом применения которых является получение информации, а также совершение действий в интересах лиц, осуществляющих такое воздействие.

Основным способом реализации методов СИ по удаленным каналам сопряжения и коммуникации являются социоинженерные (социотехнические) атаки – набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области ИБ [2]. Как правило, на практике применяются многоходовые социоинженерные атаки, при которых целевой пользователь атакуется через цепочку пользователей, с ним связанных. Результатом таких атак является значительный финансовый ущерб пользователям и организациям.

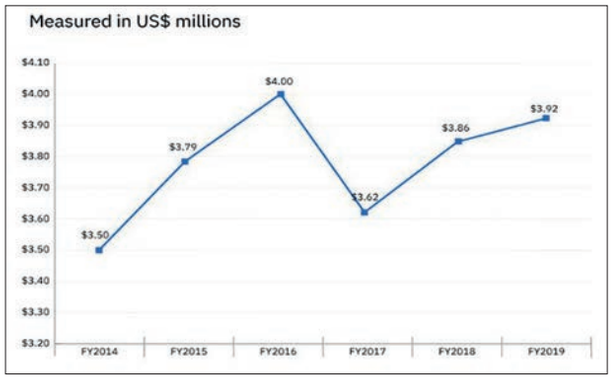


Рисунок 2 – Средняя стоимость одного инцидента утечки данных (млн долларов США) [3]

Как показывает ежегодное исследование компании IBM [3], средняя стоимость одного инцидента утечки данных в 2019 году составляет 3,92 млн долларов США. При этом за последние 5 лет рост средней стоимости утечек данных составил 12 %.

В настоящее время можно выделить следующие основные каналы проведения социоинженерных атак на основе фишинга [2]:

социальные сети: попытка манипулирования пользователем или получения информации через профиль пользователя в социальной сети;

электронная почта: фишинг-письма, которые используются для манипулирования пользователем с целью заставить его посетить вредоносный веб-сайт или открыть вредоносный файл;

телефонная связь: голосовой фишинг (vishing), используемый для непосредственного извлечения информации или убеждения цели во взаимодействии с вредоносным веб-сайтом или ранее доставленным файлом;

физический доступ: получение физического доступа к сайту или системам организации, использование обманного предлога или доставка физических носителей.

Приведенные в рамках данной статьи материалы носят исключительно научно-исследовательский характер. Исследование проводилось авторами строго в научных целях, его результаты не являются и не могут признаваться руководством к совершению каких-либо противоправных действий (fair use / fair dealing) [4]. Информация, содержащаяся в статье, получена из источников, рассматриваемых авторами как надежные. При проведении исследования авторы действовали в рамках законодательства Республики Беларусь. Авторы не несут ответственности за инциденты в сфере информационной безопасности, имеющие отношение к тематике исследования.

Содержательная постановка задачи. Согласно отчету Банка России за период 01.09.2018–31.08.2019, более 97 % хищений со счетов физических лиц и 39 % хищений со счетов юридических лиц было совершено с использованием приемов СИ [5]. Количество разделегированных доменов, с которых рассылается вредоносный код и осуществляются мошеннические действия, постоянно растет и составило 9778 шт. (рис. 3).

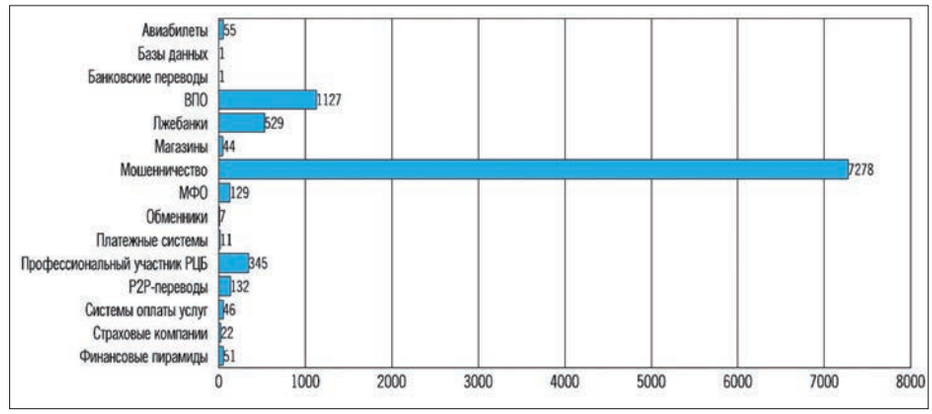


Рисунок 3 – Распределение разделегированных фишинговых доменов (данные ФинЦЕРТ Банка России за период 01.09.2018-31.08.2019 [5]

В рамках настоящей статьи выполним исследование основных технологий социоинженерных атак на пользователей сетевых ресурсов КФО, а также сформируем перечень защитных мер, позволяющих устранить или минимизировать потенциальный ущерб от их проведения.

В исследовании рассматриваются подходы к оценке успеха многоходовых (опосредованных, не прямых, не сводящихся к одному непосредственному атакующему действию злоумышленника) социоинженерных атак на пользователя с учетом параметров/показателей моделей базового профиля уязвимости цели (объекта атаки).

Результаты и обсуждение. В настоящее время имеются различные подходы по классификации и описанию структуры социоинженерных (социотехнических) атак, используемых киберпреступниками [2, 6]. Подробная академически формализованная классификация возможна только на основе полного анализа технологий проведения таких атак. Учитывая высокую латентность результатов выявления и расследования социоинженерных (социотехнических) атак, авторами на основании на данных открытых источников в качестве базовой предлагается следующая структура:

1. Сбор информации о цели атаки: ручной/автоматизированный поиск.

2. Фрейминг (Framing):

тщательный анализ собранной информации;

составление профиля уязвимостей цели – набор уязвимостей пользователя, описывающих вероятность осуществления ответных действий на социоинженерные атакующие воздействия злоумышленника;

оценка и выбор наиболее эффективных точек/узлов взаимодействия (манипулирования) с целью атаки.

3. Использование предлогов (Pretexting) – составление легенды (сценария), по которой будет осуществляться воздействие на цель, чтобы войти к ней в доверие.

4. Манипулирование: извлечение (Elicitation) и/или доставка, дальнейшая эксплуатация «полезной» нагрузки (Payload), в т. ч. с помощью вредоносного программного обеспечения (ВПО) [7].

5. Систематизация полученных данных/анализ действий.

6. Маскирование/удаление следов атаки.

Для сбора информации о цели атаки и составления профиля уязвимостей преступники, как правило, используют опорную структуру, включающую основные социально-экономические параметры/показатели пользователя ДБО КФО (табл. 1).

В настоящее время типовые методы и алгоритмы сбора и анализа информации о цели атаки достаточно подробно проанализированы и описаны [1–3, 8]. В рамках настоящей статьи остановимся на ряде современных способов, используемых для социоинженерных (социотехнических) атак.

Таблица 1 – Базовый профиль уязвимости цели (объекта атаки)

№ п/п	Характеристика объекта атаки	Детализация	Дополнительные параметры
1	Гражданство	Страна / дата приобретения гражданства	Наличие двойного гражданства (страна / дата приобретения гражданства)
2	Дата рождения	Дата / место рождения	Пол: мужской/женский
3	Место проживания / регистрации	Страна / адрес проживания (регистрации)	Дата проживания, языки для коммуникации (родной/иностранный)
4	Социальное положение	Холост / женат /разведен / вдовец (для мужчин)	Наличие детей (страна / место проживания / возраст)
5	Образование (базовое, дополнительное)	ВУЗ (специальность / квалификация), курсы повышения квалификации	Очное / заочное / дистанционное обучение. Сертификаты, ученые степени/звания
6	Место работы	Основное/дополнительное (совместительство)	Компания / должность, основные выполнение проекты
7	Увлечения (хобби)	Физические/виртуальные вещи/услуги	Степень увлечения, основные способы/каналы реализации
8	Отношение к религии	Атеист/агностик/верующий	Вероисповедание. Соблюдение ритуальных канонов
9	Социальные связи	Социальные сети/группы	Тематика диалогов, социальных предпочтений
10	Сексуальная ориентация	Принадлежность к группам сексуальных меньшинств	Степень выраженности поведения

Практический интерес для злоумышленников на этапе сбора информации представляют не только сведения с фотоизображений пользователей, которые могут стать объектами социоинженерных (социотехнических) атак, но и метаданные (формат EXIF: стандарт DFC/спецификация JEITA) [9], включенные в файлы изображений и отображаемые/редактируемые специализированным программным обеспечением (СПО). Особый интерес представляют метаданные: дата и время съемки, географические координаты и адрес места съемки (рис. 4).

Для устранения уязвимостей, связанных с НСД к EXIF-метаданным, при размещении фотоизображений в сети интернет необходимо маскировать/удалять такие данные с помощью СПО [10].

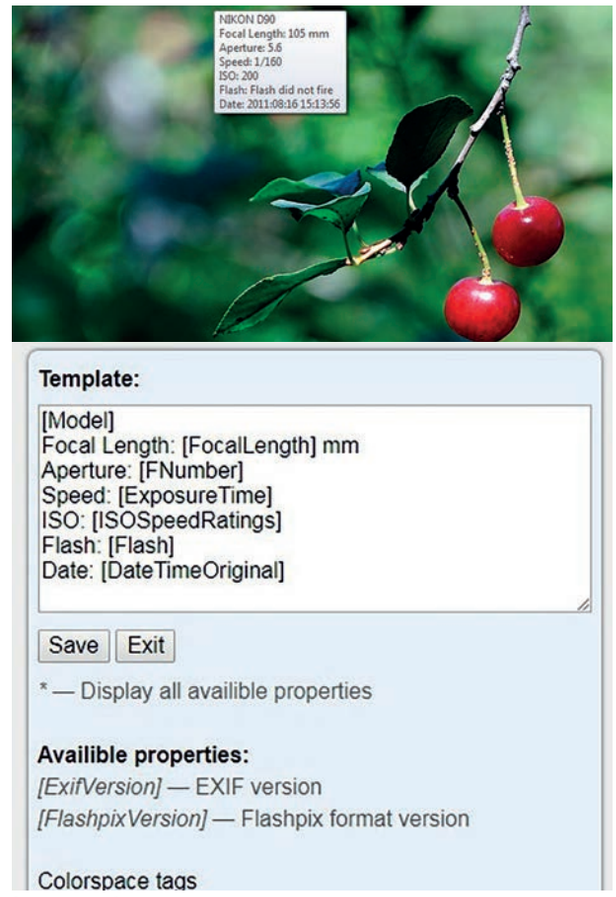


Рисунок 4 – Реализация алгоритма извлечения метаданных из фотоизображения (формат EXIF: стандарт DFC/спецификация JEITA) [11]

Для усиления эффективности реализации алгоритмов голосового фишинга (vishing) при проведении социоинженерных (социотехнических) атак преступники используют криминальные сервисы, основанные на технологиях SIP-телефонии, для подмены телефонного номера (Caller-ID) при звонках,

отправке SMS-сообщений и др. [12]. Как правило, в качестве базового клиента используется любая легальная программа SIP-клиента [13]. Коммутация звонков проходит через криминальный SIP-сервер, на котором применяются дополнительные технологии анонимизации трафика: VPN, TLS/SSL, SRTP, ZRTR (рис. 5).

Одним из наиболее эффективных методов проверки факта подмены телефонного номера (Caller-ID) по SIP-телефонии является контрольный звонок на входящий абонентский номер в сети официального оператора связи.

Оценка вероятности успеха многоходовой социоинженерной (социотехнической) атаки сводится к построению оценки вероятности сложного события, которую предлагается выполнять:

на основе модели этапов проведения социоинженерной (социотехнической) атаки с учетом детализированных параметров/показателей каждого этапа;

с использованием вероятностной модели Белла – Тревино [14]:

$$Pr_i = 1-(1-p_i)^{(N_i)} \quad (1)$$

$$P_r = 1-\prod_{i=1}^{n}(1-Pr_i), \quad (2)$$

где n – число этапов социоинженерной (социотехнической) атаки;

p_i – вероятность социоинженерной (социотехнической) атаки по i-му параметру/показателю этапа атаки;

N_i – число воздействий i-го вида параметра/показателя этапа атаки;

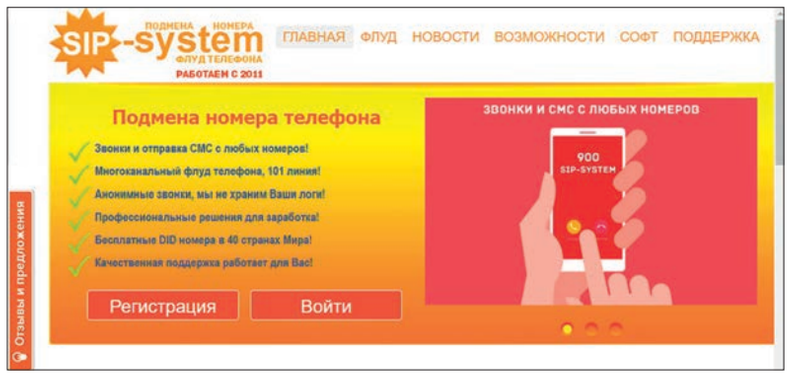
Pr_i – вероятность социоинженерной (социотехнической) атаки на конкретном ее этапе;

Pr – общая вероятность социоинженерной (социотехнической) атаки, осуществляемой по полному набору параметров/показателей всех этапов атаки.

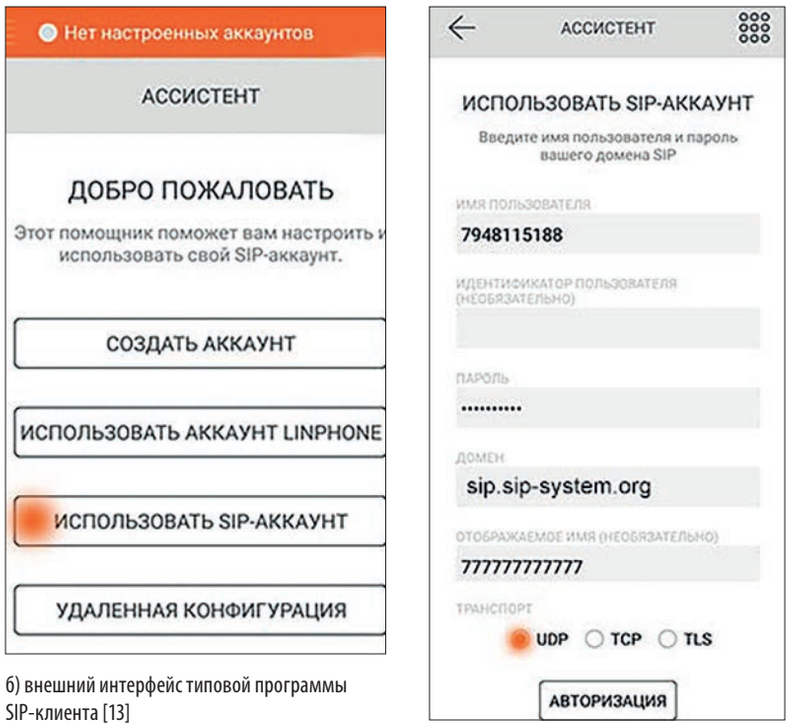
Величины p_i считаются прогнозируемыми и определяются на основе метода экспертных оценок с учетом реальных статистических данных.

Например, на этапе фрейминга (Framing) в качестве параметров/показателей предлагается модель базового профиля уязвимости цели (объекта атаки) (табл. 1). Предполагается, что определение максимального числа параметров/показателей пользователя (объекта атаки) увеличивает число способов атаки, потенциально доступных злоумышленнику.

Для оценки применимости существующих методик/алгоритмов социоинженерных (социотехнических) атак авторами статьи было проведено практическое тестовое исследование (fair use / fair dealing) [4]. В качестве объектов атаки были выбраны два пользователя ДБО двух разных КФО [15] (согласие пользователей ДБО КФО на исследование получено, и проведен дополнительный инструктаж, Ф. И. О. пользователей заменены порядковыми номерами, фишинг эмулировал адресные данные сервисов КФО, срок возможного



а) сервис криминальной SIP-телефонии [12]



б) внешний интерфейс типовой программы SIP-клиента [13]

Рисунок 5 – Реализация алгоритма голосового фишинга (vishing) на основе технологий SIP-телефонии

Таблица 2 – Результаты тестовой социоинженерной (социотехнической) атаки

№ польз-ля	Получение информации по базовому профилю уязвимости цели (таблица 1), %	Доставка адресного фишингового сообщения на e-mail [16]	Фиксация (Honeypot) перехода на фишинговый ресурс [17, 18]	Звонок с подменой телефонного номера (Caller-ID) по SIP-телефонии [19]
1	80	+	–	+
2	55	+	+	+

проведения цикла атаки – до десяти дней). Оценка полноты информации по базовому профилю уязвимости цели атаки осуществлялась на основе метода экспертных оценок.

По результатам тестовой социоинженерной (социотехнической) атаки минимум один из пользователей ДБО КФО мог быть атакован с помощью ВПО и введен в заблуждение голосовым фишингом (vishing) с целью дальнейшего манипулирования, а также мог понести потенциальный финансовый ущерб (табл. 2).

Основным способом снижения эффективности социоинженерных (социотехнических) атак является систематическое обучение и повышение осведомленности пользователей ДБО КФО о безопасных методах пользования такими сервисами путем эмуляции реальных атак [20].

Расследование киберпреступлений, основанных на социоинженерных (социотехнических) атаках, является сложным и затратным процессом. В связи со значительным ростом количества киберпреступлений правоохранительные органы вынуждены постоянно запрашивать информацию у телекоммуникационных провайдеров и сервисов для раскрытия пользовательских данных (рис. 6) [21]. При этом за предоставление информации/реализацию ордеров, например, компания Google с 13 января 2020 года с разрешения правительства США взимает плату 45–245 долларов США [22].

Заключение. На основании проведенного исследования основных технологий социоинженерных (социотехнических) атак на пользователей сетевых ресурсов КФО можно сделать следующие выводы:

1. В настоящее время социоинженерные (социотехнические) атаки носят массовый характер и имеют высокую латентность результатов выявления/расследования. В ходе исследования авторами описана базовая структура проведения таких атак, которая включает детализацию каждого из пяти ее этапов.

2. Предложен подход к оценке вероятности успеха многоходовой социоинженерной (социотехнической) атаки (формулы 1, 2), а также описана модель базового профиля уязвимости цели (объекта атаки) (табл. 1).

3. Для анализа эффективности алгоритмов/подходов, используемых киберпреступниками, проведена тестовая социоинженерная (социотехническая) атака на двух типовых пользователей ДБО КФО (fair use / fair dealing) [4] (табл. 2).

4. Предложены рекомендации для противодействия ряду способов, используемых для проведения социоинженерных (социотехнических) атак.

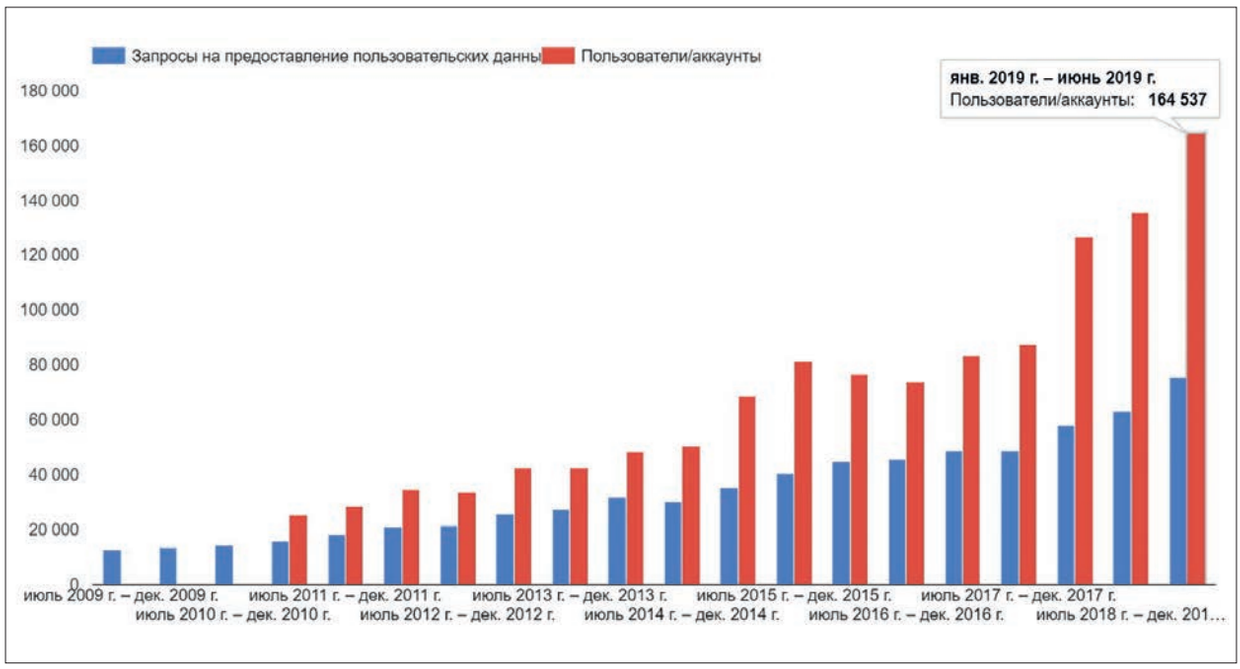


Рисунок 6 – Запросы личной информации от государственных органов в Google [21]

ЛИТЕРАТУРА

1. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году // cbr.ru [Электрон. ресурс]. – 2000–2020. – Режим доступа: http://www.cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/. – Дата доступа: 20.01.2020.
2. **Абрамов, М.В.** Методы и алгоритмы анализа защищенности пользователей информационных систем от социоинженерных атак: оценка параметров моделей: дис. ... к-та технич. наук: 05.13.19 / М.В. Абрамов. – Санкт-Петербург, 2018. – 232 л.
3. 2019 Cost of a Data Breach Report / securityintelligence.com [Электрон. ресурс]. – 2020. – Режим доступа: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/. – Дата доступа: 21.01.2020.
4. Coders' Rights Project Reverse Engineering FAQ // eff.org [Электрон. ресурс]. – 2020. – Режим доступа: https://www.eff.org/ru/issues/coders/reverse-engineering-faq/. – Дата доступа: 22.01.2020.
5. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (01.09.2018 – 31.08.2019) // cbr.ru [Электрон. ресурс]. – 2000–2020. – Режим доступа: http://www.cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF/. – Дата доступа: 23.01.2020.
6. Hi-Tech Crime Trends 2019/2020 // group-ib.ru [Электрон. ресурс]. – 2003–2020. – Режим доступа: https://www.group-ib.ru/resources/threat-research/2019-report.html/. – Дата доступа: 24.01.2020.
7. Рынок преступных киберуслуг // ptsecurity.com [Электрон. ресурс]. – 2002-2020. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/darkweb-2018/. – Дата доступа: 24.01.2020.
8. Cyber's Most Wanted // fbi.gov [Электрон. ресурс]. – 2020. – Режим доступа: https://www.fbi.gov/wanted/cyber/. – Дата доступа: 25.01.2020.
9. JEITA CP-3451 / Exchangeable image file format for digital still cameras: Exif Version 2.2 // exif.org [Электрон. ресурс]. – 2020. – Режим доступа: http://www.exif.org/Exif2-2.PDF/. – Дата доступа: 25.01.2020.
10. EXIF. Технические данные фотографии: как их посмотреть и удалить // prophotos.ru [Электрон. ресурс]. – 2007-2020. – Режим доступа: https://prophotos.ru/lessons/19195-exif-tehnicheskie-dannye-fotografii-kak-ih-posmotret-i-udalit/. – Дата доступа: 26.01.2020.
11. Exponator Live! // chrome.google.com [Электрон. ресурс]. – 2020. – Режим доступа: https://chrome.google.com/webstore/detail/exponator-live/kbnckhjhgepdfhgnklcffik hfndhfgfc/. – Дата доступа: 26.01.2020.
12. Подмена номера телефона // sip-system.com [Электрон. ресурс]. – 2011–2020. – Режим доступа: https://sip-system.com/. – Дата доступа: 27.01.2020.
13. Linphone // play.google.com [Электрон. ресурс]. – 2020. – Режим доступа: https://play.google.com/store/apps/details?id=org.linphone&hl=ru/. – Дата доступа: 27.01.2020.
14. Bell D. C., Trevino R. A. Modeling HIV Risk [Epidemiology] // J. Acquir Immune Defic Syndr. 1999. Vol. 22, N 3. P. 280–287.
15. Банковская система // nbrb.by [Электрон. ресурс]. – 2000–2020. – Режим доступа: https://www.nbrb.by/system/banks/list. – Дата доступа: 28.01.2020.
16. Anonymous Email // anonymousemail.me [Электрон. ресурс]. – 2020. – Режим доступа: https://anonymousemail.me//. – Дата доступа: 28.01.2020.
17. Honeypots for Detecting Network Threats // securitytrails.com [Электрон. ресурс]. – 2020. – Режим доступа: https://securitytrails.com/blog/top-20-honeypots/. – Дата доступа: 28.01.2020.
18. Spam Honeypot Tool // github.com [Электрон. ресурс]. – 2020. – Режим доступа: https://github.com/miguelraulb/spamhat/. – Дата доступа: 29.01.2020.
19. Black Wolf // black-wolf.tech [Электрон. ресурс]. – 2020. – Режим доступа: https://black-wolf.tech/#test/. – Дата доступа: 30.01.2020.
20. Kaspersky Automated Security Awareness Platform // asap.kaspersky.com [Электрон. ресурс]. – 2020. – Режим доступа: https://asap.kaspersky.com/ru/. – Дата доступа: 30.01.2020.
21. Запросы личной информации // transparencyreport.google.com [Электрон. ресурс]. – 2020. – Режим доступа: https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:;time:&lu=user_requests_report_period. – Дата доступа: 30.01.2020.
22. Have a Search Warrant for Data? Google Wants You to Pay // nytimes.com [Электрон. ресурс]. – 2020. – Режим доступа: https://www.nytimes.com/ 2020/01/24/technology/google-search-warrants-legal-fees.html?fbclid=IwAR1RQnnLll25Ps_ 0ZQ6EiRgIauLu-zxLN3u0mAuY4LLrdrOK60AaH8pCFYQ/. – Дата доступа: 30.01.2020.

The study of technologies for conducting socio-engineering (sociotechnical) attacks on users of remote banking services (RBS) of credit and financial organizations (CFO) was performed. The basic structure of such attacks is described. Approaches to counteracting algorithms/approaches used by cybercriminals are proposed.

Keywords: *RBS, CFO, socioengineering (sociotechnical) attack, malicious software.*

Получено 03.02.20.