4. Есенкулова С.А. Упрощенный порядок судебного разбирательства в уголовном судопроизводстве (по материалам Кыргызской Республики и Российской Федерации): Автореф. дис. … канд. юрид. наук. - М., 2013.
5. Ивенский А.И. Приговор - акт правосудия, осуществляемого в общем и особом порядках судебного разбирательства: Автореф. дис. … канд. юрид. наук. - Саратов, 2006.
6. Кищенков А.В. Упрощенные производства: проблемы теории, законодательного регулирования и правоприменения: Автореф. дис. … канд. юрид. наук. - Владивосток, 2010.
7. Колоколов Н.А. В поисках convenient criminal law // Уголовное судопроизводство. - 2014. - № 1.
8. Лагуткина Н.Б. Особый порядок принятия судебного решения при согласии обвиняемого с предъявленным обвинением // Наука и современность. - 2013. - № 21.
9. Мурашкин И.Ю. Заявление ходатайства о рассмотрении уголовного дела в особом порядке // Вестник Омского юридического института. - 2011. - № 4(17).
10. Особый порядок судебного разбирательства: проблемы теории и практики: монография / науч. ред. А.Ф. Ефремов. - Саратов, 2008.
11. Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. Эл. ресурс. Режим доступа: http://www.cdep.ru (дата обращения: 23.02.2021 г.)
12. Постановление Пленума Верховного Суда РФ от 05.12.2006 № 60 (в ред. от 22.12.215) «О применении судами особого порядка судебного разбирательства уголовных дел» // Бюллетень Верховного Суда РФ. - 2007. - № 2.
13. Правосудие в современном мире: монография / Под ред. В.М. Лебедева, Т.Я. Хабриевой. - М.: Норма, Инфра-М, 2012.
14. Щербина Е.В. Основания для рассмотрения уголовного дела в особом порядке // Известия Оренбургского государственного аграрного университета. - 2013. - № 4(42).

Демченко А.А., Мамин А.С.

Методика проведения отдельных мероприятий, связанных с несанкционированным доступом к системам дистанционного банковского обслуживания

Белгородский государственный национальный исследовательский университет (Россия, Белгород)

doi: 10.18411/lj-04-2021-226

Аннотация

Данная статья направлена на рассмотрение и анализ несанкционированного доступа к системам дистанционного банковского обслуживания. Авторы уделяют внимание правовым проблемам в данной сфере, а также предлагают решение данной проблемы.

Ключевые слова: дистанционное банковское обслуживание, вредоносная программа, денежные средства.

Abstract

This article is aimed at reviewing and analyzing unauthorized access to remote banking systems. The authors pay attention to the legal problems in this area, and also offer a solution to this problem.

Keywords: remote banking, malware, money.

Анализ практики органов внутренних дел в области несанкционированного доступа к системам дистанционного банковского обслуживания позволяет наглядно рассмотреть схему такого алгоритма. В случае попадания на пользовательский персональный компьютер, вредоносное программное обеспечение проводит анализ составляющих носителя жесткого магнитного диска, ищет определенные виды файлов по сигнатурам, которые входят в состав программного обеспечения систем дистанционного банковского обслуживания. Однако, если подобных файлов не обнаружится, то вредоносная программа ищет пути распространения через локальные сети и уже там продолжает действовать. При обнаружении результата в зависимости от найденного программного продукта, представленного разработчиками систем дистанционного банковского обслуживания, вносит дополнительные модули

программного обеспечения, при этом сообщая злоумышленнику о том, что на анализируемым персональном компьютере обнаружено программное обеспечение определенного банка. Подобная вредоносная программа собирает и «запоминает» данные о клиенте банка, пароли, вводимые клиентом, лог-файлы действий пользователя, его переписку и т.д.

Особо важной информацией являются сведения об остатке денежных средств, находящихся на счете клиента, т.к. на основе таких данных производится построение анализа хода денежных средств и их использование. Злоумышленнику необходим момент аккумуляции максимальной суммы денежных средств на счете клиента, как правило, в такой момент он совершает попытку несанкционированного перевода денежных средств.

Исходя из некоторых технических подробностей следует отметить, что в большинстве случаев в тот момент, когда злоумышленник вводит команду о подобном переводе денежных средств, данная команда поступает через цепочку заранее скомпрометированных компьютеров, находящихся в разных местах планеты, данная операция делает проблематичным установление реального лица, совершившего инцидент. Как правило, на серверах банковской системы установлены необходимые настройки фильтров безопасности, в результате которых администрирование клиентом системы дистанционного банковского обслуживания будет возможно только с определенного адреса в сети выделенного компьютеру или физического адреса (IP - адрес и MAC - адрес) оговоренного ранее с пользователем или с диапазона таких адресов, возможно, выделенных интернет - провайдеру или одному из сегментов сети Интернет. В таком случае злоумышленник пытается подобрать и осуществить несанкционированный доступ к конкретному персональному компьютеру.

При осуществлении несанкционированного перевода сравнительно небольшой суммы денежных средств со счета скомпрометированного юридического лица на заранее приготовленный счет физического лица подельник или сам злоумышленник, который получает денежные средства из банкомата знает о примерном времени перевода, в таком случае, он может спланировать свои действия досконально. В некоторых случаях к такому счету привязывается абонентский номер оператора сотовой сети связи, и при получении сообщения о пополнении счета лицо обналичивает переведенные суммы денежных средств. Основным критерием при получении наличных лицом из банкомата является максимальная анонимность, на это влияет и выбор расположения банкомата, проходимость места, освещение и его видео оснащенность. На практике известны не многие случаи, когда видео безопасность обеспечивается качественно, когда удается распознать и выявить отличительные черты лица. При этом наблюдается извечная проблема периода времени хранения записанного материала из-за количества объектов наблюдения и времени наблюдения делает многие инциденты не раскрытыми.

Говоря об оперативно-розыскных мероприятиях, которые возможно проводить при получении сообщения об инциденте, связанном с несанкционированным доступом к системе дистанционного банковского обслуживания следует отнести мероприятия, направленные на обеспечение связи с банком, обслуживающим клиента, со счета которого не санкционированно списаны денежные средства, для того, чтобы принять меры к приостановки не согласованной операции по переводу денежных средств. Руководство банка, как правило, заинтересовано в сохранении своей репутации и охотно идут на встречу в вопросах разрешения инцидента с правоохранительными органами. Данный этап в раскрытии данного рода преступления является перспективным, так как с его помощью представляется возможным вернуть похищенные денежные средства.

Имеющим важное значение мероприятиям является действия после инцидента, направленные на обеспечение сохранности информации на носителях жестких магнитных дисков скомпрометированного компьютера, на котором установлено программное обеспечение системы дистанционного банковского обслуживания. Для

этого при получении сообщения о рассматриваемом инциденте необходимо принять меры об уведомлении лиц, администрирующих компьютер, на которым был установлен программный продукт, о невозможности дальнейшего его использования, отключения его от сети Интернет и питания. Необходимо пояснить, что ни при каких условиях не нужно пытаться запускать компьютер, так как с каждым разом логическая структура жесткого диска, а, следовательно, и необходимая для исследования криминалистическая информация будет безвозвратно потеряна, восстановить причинно-следственную связь совершенного инцидента не представится возможным. Как можно быстрее необходимо назначить и истребовать исследование, которое может дать необходимую информацию для результативного и качественного расследования преступления.

После истребования сведений у банковской структуры о статистике подключений клиента к серверу банка необходимо выявить неизвестные адреса пользователей сети, далее, при наличии таких, принять меры для их установления.

Целесообразно истребовать сведения от интернет- провайдера клиента с целью получения статистики подключения к сети интернет его абонента. При обработке сведений необходимо обратить внимание на временные интервалы подключения, физические адреса устройств, а также подключения к выделенному абоненту других пользователей с других адресов сети Интернет. При обработке допускается возможность установить цепочку, по которым злоумышленник осуществлял администрирование, это могут быть проверочные соединения или периоды времени самого несанкционированного администрирования, в ходе которого были переведены денежные средства. Период исследуемых сведений лучше расширить, так как проверочные соединения злоумышленника могут иметь спонтанный и хаотичный характер.

Для понимания работы вредоносного программного обеспечения необходим подробный опрос пользователя, который непосредственно администрировал систему дистанционного банковского обслуживания с целью выявления поведения операционной системы до инцидента и в его момент.

Следует признать, что рассмотренная в настоящей работе методика проведения отдельных мероприятий, связанных с несанкционированным доступом к системам дистанционного банковского обслуживания представляет собой правовую проблему в ближайшее время вряд ли может быть легко разрешена и, следовательно, борьба с хищениями денежных средств с использованием вредоносных программ будет по-прежнему затруднена. Для улучшения сложившейся ситуации, по мнению автора, необходимо создание целенаправленной деятельности правоохранительных органов. В частности, нуждаются в совершенствовании нормы административно-процессуального, уголовно-процессуального законодательства. Требуются руководящие разъяснения высшей судебной инстанции по некоторым сложным вопросам, касающимся определения места производства предварительного расследования по уголовным делам о таких преступлениях. Необходима разработка методологии проведения экспертными подразделениями органов внутренних дел исследований носителей информации, подвергшихся воздействию вредоносных компьютерных программ, а также совершенствование деятельности самих экспертных подразделений по проведению судебных компьютерно-технических экспертиз. Отдельными задачами являются разработка централизованного учета оперативной информации, поступающей в процессе борьбы с преступлениями в сфере компьютерной информации, а также организация информационно-аналитической работы.

***

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru. (дата обращения:15.01.2021).

2. О банках и банковской деятельности: Федеральный закон от 2.12. 1990 г. № 395-I (ред. от 30.12.2020)// Ведомости съезда народных депутатов РСФСР, 06.12. 1990 г. № 27 ст. 357.
3. О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10 июля 2002 г. № 86-ФЗ (01.01.2021)// Собрание законодательства Российской Федерации,15 июля 2002 г. № 28 ст. 2790
4. О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ// Собрание законодательства Российской Федерации, 04.07. 2011 г. № 27 ст. 3872
5. Аникин А. В. Защита банковских вкладчиков. Российские проблемы в свете мирового опыта. М., 2017. С. 30.
6. Тавасиев, А.М. Банковское регулирование и надзор в 2-х частях. Часть 2. Технологии обслуживания клиентов. Учебник для СПО / А.М. Тавасиев. - М.: Юрайт, 2014. - 449 с.

Елесина И.Г.[1], Воронов А.С.[2], Елесина Е.А.[3]

Проблемы регулирования розыска и этапирования лиц, скрывающихся от органов дознания, следствия и суда

[1]Санкт-Петербургский университет МВД России
[2]Санкт-Петербургский государственный университет аэрокосмического приборостроения
[3]Российский государственный университет правосудия
(Россия, Санкт-Петербург)

doi: 10.18411/lj-04-2021-227

Аннотация

В статье представлены проблемы организации розыска лиц, подозреваемых и обвиняемых в совершении преступлений, скрывающихся от органов дознания, следствия и суда, совершивших побег из-под стражи, осужденных, уклоняющихся от исполнения наказания. Рассмотрены проблемы правового регулирования конвоирования таких лиц в регион совершения преступления для проведения следствия и суда.

Ключевые слова: розыск, преступление, подозреваемые и обвиняемые, лица, скрывающиеся от следствия и суда, оперативно-розыскная деятельность, конвоирование.

Abstract

The article presents the problems of organizing the search for persons suspected and accused of committing crimes hiding from the bodies of inquiry, investigation and court, who escaped from custody, convicted, evading the execution of punishment. The problems of legal regulation of escorting such persons to the region of committing a crime for investigation and trial are considered.

Key words: search, crime, suspects and accused, persons hiding from investigation and trial, operational-search activity, escorting.

На современном этапе розыск лиц, подозреваемых и обвиняемых в совершении преступлений, скрывающихся от органов дознания, следствия и суда, совершивших побег из-под стражи, осужденных, уклоняющихся от исполнения наказания, является актуальной правовой и практической проблемой.

В первую очередь это обусловлено территориальным фактором – значительной по площади территорией Российской Федерации, малонаселенными территориями Сибири, Дальнего Востока, и, следовательно, значительно отдаленных друг от друга дислокаций правоохранительных органов.

С точки зрения правовой регламентации проблема розыска лиц, скрывающихся от органов дознания, следствия и суда, обусловлена рядом неурегулированных нормативными правовыми актами организации процедуры сбора и систематизации информации о таких лицах, межведомственного взаимодействия органов дознания,