

МВД России

Федеральное государственное казенное учреждение
дополнительного профессионального образования
«Всероссийский институт повышения квалификации сотрудников
Министерства внутренних дел Российской Федерации»

М. Ю. Литвинов, В. И. Алескеров

**ПРОТИВОДЕЙСТВИЕ
СОВРЕМЕННЫМ ВИДАМ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

Научно-практическое пособие

Часть 2

2-е издание, переработанное и дополненное

Домодедово
ВИПК МВД России
2026

ББК 67.408.135

Л 64

Авторский коллектив:

М. Ю. Литвинов, кандидат технических наук; **В. И. Алескеров**, кандидат юридических наук, доцент.

Рецензенты:

А. А. Курносенко – первый заместитель Министра внутренних дел Российской Федерации генерал-лейтенант полиции;

С. Н. Лебедев – заместитель Министра – начальник СД МВД России генерал-полковник полиции;

В. В. Голованов – начальник ГУУР МВД России генерал-лейтенант полиции;

О. В. Ильиных – начальник ГУПЭ МВД России генерал-лейтенант полиции;

О. А. Баранов – начальник ГУ МВД России по г. Москве генерал-лейтенант полиции;

В. К. Пауков – начальник ГУ МВД по Московской области генерал-лейтенант полиции;

С. А. Синенко – начальник Академии управления МВД России генерал-лейтенант полиции.

Л 64 Противодействие современным видам преступлений, совершаемых в условиях цифровизации : научно-практическое пособие : в 3 частях : 2-е издание, переработанное и дополненное / М. Ю. Литвинов, В. И. Алескеров. – Домодедово : ВИПК МВД России, 2026.

Часть 2. – 2026. – 162 с.

В научно-практическом пособии раскрываются уголовно-правовая и криминалистическая характеристики преступлений, совершаемых в условиях цифровизации. Рассматриваются проблемные вопросы раскрытия преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации, особое внимание уделено раскрытию преступлений в системе дистанционного банковского обслуживания и преступлений террористического характера и экстремистской направленности.

Авторами даны понятия цифровизации, биллинга, идентификации, технического канала связи, телекоммуникационной сети, тайминга и др., с учетом криминалистического и оперативно-розыскного аспектов; впервые рассмотрены некоторые способы маскирования оперативно значимой информации.

Данное пособие предназначено для сотрудников подразделений специальных технических мероприятий, других оперативных подразделений органов внутренних дел и правоохранительной системы Российской Федерации. Будет полезно курсантам, адъюнктам, профессорско-преподавательскому составу высших учебных заведений юридического профиля правоохранительной системы Российской Федерации.

ББК 67.408.135

© ВИПК МВД России, 2026

Глава IV.

Раскрытие преступлений, совершаемых в системе дистанционного банковского обслуживания

В настоящее время в мире происходят экономические преобразования динамического характера, которые влияют не только на политический сегмент, но и на быстро развивающуюся сферу информационных-телекоммуникационных и компьютерных технологий. Информационные потоки, вливающиеся во все сферы жизнедеятельности современного общества, придают возможности бурного развития социального обеспечения, финансов, экономики, медицины, образования, всевозможных научных исследований на всех направлениях. Несмотря на эту положительную сторону, как всякое новое веяние, преобразования, кроме масштабных революционных изменений, неизбежно влекут за собой и некоторые нежелательные последствия. К таким последствиям мы можем отнести преступления, совершаемые в сфере телекоммуникаций и компьютерной информации. Одним из разновидностей таких преступлений являются преступления, совершаемые в системе дистанционного банковского обслуживания¹, статистика которых из года в год показывает геометрическую прогрессию, а ущерб от данного вида преступлений, к нашему сожалению, велик (диаграмма 1).



Диаграмма 1. Количества преступлений, совершаемых в системе ДБО²

¹ Далее – «ДБО».

² Данные взяты из статистических сведений ФКУ «Главный информационно-аналитический центр МВД России».

За последние годы проводится целый ряд глубоких исследований преступлений данной направленности, на основе чего подготовлены доклады, отчеты, статьи и рекомендации, но во всех перечисленных документах прослеживается четкое высказывание, что преступления, совершаемые в системе ДБО, являются преступлениями, относящимися к разновидностям киберпреступлений. А если выражаться еще точнее, то данный вид преступлений можно отнести и к **компьютерно-экономическим** преступлениям. Повсеместное использование технологических возможностей информационно-телекоммуникационных сетей и компьютерной информации в глобальной сети Интернет порождает благоприятные условия, способствующие осуществлению преступного замысла среди лиц, совершающих преступления в системе ДБО. Данное обстоятельство не может не вызывать тревогу у сотрудников оперативных подразделений, призванных вести активную и целенаправленную работу по противодействию данному виду преступлений, так как в большинстве случаев лица, совершающие этот вид преступлений, остаются без соответствующего наказания.

Киберпреступность, ее рост являются следствием продолжающейся глобализации внедрения информационно-телекоммуникационных технологий и появления международных компьютерных сетей. С масштабным ростом информационных систем в различных областях деятельности возрастает и их применение в целях совершения преступлений. В этой связи можно утверждать, что электронная революция дала толчок преступности, использующей возможности информационно-телекоммуникационных сетей для извлечения прибыли. Появились новые формы и виды преступлений, представляющие угрозу для граждан, предприятий, организаций, государств.

Алексей Лунин, автор статьи *«Как не стать жертвой мошенников?»*, не зря упоминает о том, что воры-психологи все чаще крадут деньги с банковских карт пенсионеров. Так по оценкам аналитиков, в 2017 году мошенники с помощью социальной инженерии похитили с банковских карт жителей нашей страны почти 750 млн. руб., причем большая часть пострадавших – пенсионеры. Он же в своей статье *«Реально ли победить киберпреступность?»* приводит следующую информацию: «Сумму ущерба мировой экономике от действий киберпреступников в 2017 году аналитики экономического форума в Давосе оценили в 1 трлн. долл. США»³. В России потери тоже ощутимы. «Статистика говорит о 150-200 млн. руб. в 2017 году, но, видимо, это только официально зафиксированные и как-то расследованные инциденты. Оценка аналитиков, касающаяся всей страны, – 550-600 млрд. руб. Прогноз ежегодных возможных потерь может

³ «Аргументы и факты» № 26, 2018 (www.aif.ru).

составить 1 трлн. руб.», – приводит красноречивые цифры заместитель председателя правления Сбербанка России Станислав Кузнецов.

В начале июля 2018 г. Сбербанк провел в Москве Международный конгресс по безопасности в сфере информационных технологий. Это один из первых шагов России к созданию всемирной системы обмена информацией о преступлениях в сфере информационных технологий и борьбы с лицами, их совершающими. Разработчики антивирусных программ, руководители банков, представители Интерпола и правоохранительных органов обменивались опытом и обсуждали общие правила противодействия угрозам в сфере информационных технологий. Как организатор конгресса Сбербанк решил открыто показать свои методы работы. Защищая своих клиентов, он действует по **четырем направлениям**:

Первое – безопасность центральных банковских систем, где хранятся все сведения о счетах. Второе – разработка новых финансовых продуктов, в программный код которых уже на старте проекта зашиваются базовые принципы безопасности. Третье – анализ нестандартных действий и ошибок клиентов. Для этого используется специальная система антифрода с искусственным интеллектом, которая способна выявить и не допустить до 97% мошеннических операций. Четвертое – тщательное расследование каждой кибератаки, нацеленное на выявление мошенников⁴.

В целях консолидации усилий в противодействии электронной преступности Советом Европы была разработана Конвенция о киберпреступности, ставшая первым международно-правовым документом в этой области. На заседании в Будапеште 23 ноября 2001 г. министрами иностранных дел Европейского Сообщества принята Европейская Конвенция по борьбе с компьютерной преступностью, а сегодня к этой конвенции присоединилось более 40 стран⁵.

Мошенничество является одним из самых распространенных криминальных проявлений на территории Российской Федерации. Прежде всего, это связано с тем, что российское законодательство придает особое значение проблемам усиления ответственности за различные виды мошеннических действий. В период с 2003 по 2011 гг. в ст. 159 УК РФ внесены значительные изменения и дополнения, усиливающие уголовную ответственность за данный вид хищения. *В 2012 году на основании Федерального закона от 29 ноября № 207-ФЗ в Уголовный кодекс введены шесть новых видов мошеннических действий, в том числе:*

- ст. 159.1 – мошенничество в сфере кредитования;
- ст. 159.2 – мошенничество при получении выплат;

⁴ «Аргументы и факты» № 26, 2018 ([www/aif.ru](http://www.aif.ru)).

⁵ Тарасов А.М. Электронное правительство и информационная безопасность: учебное пособие. – СПб: ГАЛАРТ, 2011.

- ст. 159.3 – мошенничество с использованием электронных средств платежа⁶;
- ст. 159.4 – мошенничество в сфере предпринимательской деятельности⁷;
- ст. 159.5 – мошенничество в сфере страхования;
- ст. 159.6 – мошенничество в сфере компьютерной информации.

В соответствии со ст. 159 Уголовного кодекса Российской Федерации, мошенничеством признается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При мошенничестве обман, или злоупотребление доверием, является способом завладения чужим имуществом. Особенностью такого вида хищения, как мошенничество, является то, что в результате обмана потерпевший сам передает преступнику имущество, при этом добровольность передачи имущества является мнимой, поскольку обусловлена совершенным в отношении потерпевшего обманом, введением его в заблуждение. Любая форма обмана и злоупотребления доверием, в целом, сводится к тому, что виновный при осуществлении своих действий создает у потерпевшего уверенность в правомерности или выгоды для него передачи имущества или права на него. С развитием современного общества, появлением прогрессивных технических возможностей, научными открытиями и изобретениями, к сожалению, все чаще выявляются новые виды мошеннических действий, которые в последнее время активно совершенствуются.

Мошенничество – это общественно опасное деяние, которое причиняет не только имущественный вред гражданам, но и подрывает доверие между людьми, разрушает нравственные устои общества в целом. Как показывает практика, за последнее время нашел активное распространение такой вид преступления, как мошенничество с использованием средств сотовой телефонной связи и ДБО. С 2008 года данные виды мошенничества начали активно совершенствоваться и получили достаточно широкое распространение на территории Российской Федерации. Среди большого многообразия видов мошенничества данные виды получили название «телефонное» мошенничество и мошенничество в сфере ДБО, поразив практически все регионы России.

«Телефонное» мошенничество можно охарактеризовать как мошенничество, при котором деньги похищаются у потерпевшего под различными предложениями: путем обмана или введения в заблуждение последнего, с помощью средств сотовой телефонной связи. По данным ФКУ «ГИАЦ МВД России», в структуре преступности за период 2018–2023 гг. мошенничество занимает – 10,8%, что составляет пятую часть от всего объема хищений. Особо следует отметить, что в 2023 году, несмотря на предпринимаемые меры противодействия, произошел рост рассматриваемых видов преступлений на 9,8%. В настоящее время количество рассматриваемых видов преступлений продолжает расти.

⁶ В ред. Федерального закона от 23 апреля 2018 г. № 111-ФЗ.

⁷ В соответствии с постановлением Конституционного Суда Российской Федерации от 11 декабря 2014 г. № 32-П статья 159.4 УК РФ с 12 июня 2015 года утратила силу.

4.1. Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых в системе дистанционного банковского обслуживания

Статистика свидетельствует, что хищения денежных средств, совершенных с использованием вредоносных программ, составляют незначительную часть в структуре преступности. Однако ущерб, причиненный ими, по мнению ведущих специалистов в этой области, настолько велик, что сразу не поддается конкретной оценке. Используемые злоумышленниками замаскированные способы преступных действий и осуществление адекватного противодействия расследованию существенно затрудняет ведение борьбы с преступлениями рассматриваемого вида. Каждая вновь возникшая ситуация требует индивидуального подхода и актуализации необходимых вопросов, необходимых в ходе решения раскрытия хищений денежных средств, совершаемых в системе ДБО. ДБО – технологии предоставления банковских услуг на основании распоряжений, передаваемых клиентом без его визита в банк, чаще всего с использованием компьютерных и телефонных сетей (рис. 1). В каждой конкретной ситуации рассматриваемого вида преступлений присутствует **корысть**, и, как результат, происходит безвозмездное противоправное изъятие денежных средств и оборот их в пользу участника преступления.



Рис. 1. Дистанционное банковское обслуживание (ДБО)

В связи с вопросами, возникшими в судебной практике при рассмотрении уголовных дел о хищениях, Пленум Верховного Суда Российской Федерации дал некоторые разъяснения⁸, но данные разъяснения лишь фрагментарно затронули вопросы квалификации хищения денежных средств в системе ДБО (с использованием электронных средств платежа). Кроме того, данные разъяснения были даны до изменений действующего уголовного законодательства и законодательства в сфере банковской деятельности, связанных с регламентацией безналичных расчётов. В связи с чем, в практической деятельности судов, а также следственных органов остаются множество неразрешенных вопросов⁹.

Одним из распространенных способов хищений денежных средств с лицевых счетов клиентов банка может быть преступный сговор сотрудников кредитных организаций, уполномоченных осуществлять различного вида услуги в системе ДБО, или иных лиц, наделенных правами и возможностями доступа к компьютеру, подключенному к системе ДБО (рис. 2).

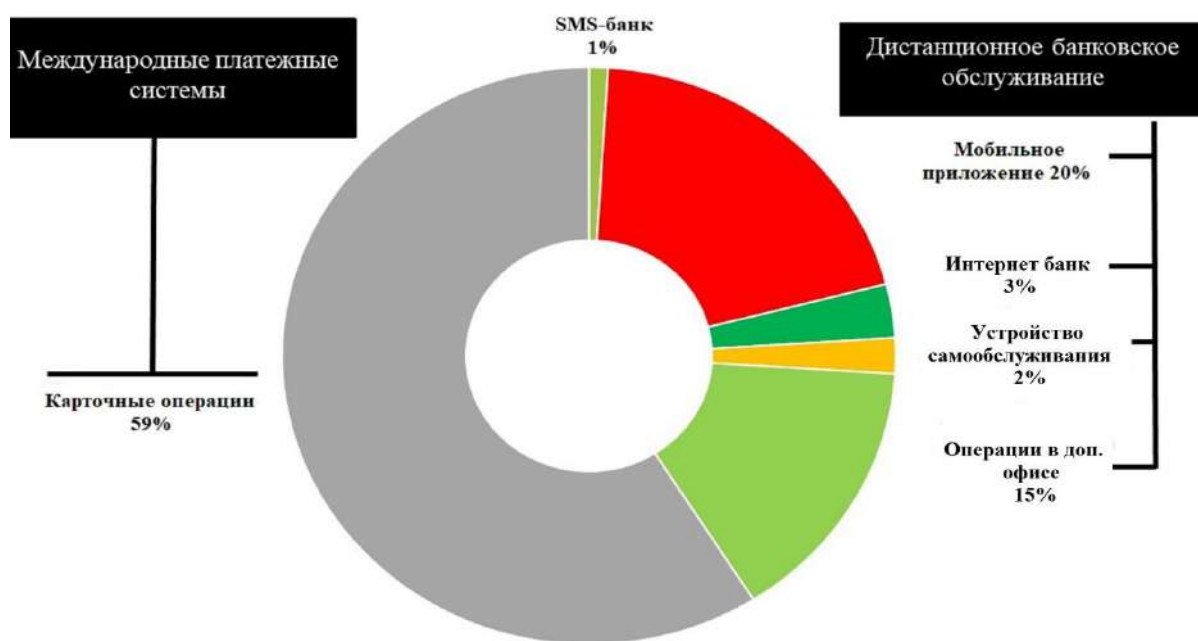


Рис. 2. Удаленные каналы обслуживания как объект преступного посягательства

⁸ О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 // Бюллетень Верховного Суда Российской Федерации. 2003. № 2; О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 // Бюллетень Верховного Суда Российской Федерации. 2008. № 2.

⁹ Шмонин А.В., Баранов В.В. Организация выявления, раскрытия и расследования хищений денежных средств в системе дистанционного банковского обслуживания: учебно-практическое пособие / под науч. ред. доктора юридических наук, профессора А.В. Шмони́на. Москва : Академия управления МВД России, 2014.

В зависимости от складывающейся обстановки, а также способа совершения хищений денежных средств в системе дистанционного банковского обслуживания, согласно нормам ст. 158, 159.6 УК РФ, преступления могут совершаться в виде краж и мошенничества в сфере телекоммуникационных систем.

Исходя из криминогенной обстановки, авторы работы считают необходимым рассмотрение ст. 160 УК РФ, так как преступления в системе ДБО при определенных ситуациях можно рассматривать в виде присвоения либо растраты.

Предлагаем рассмотреть вышеуказанные виды преступлений.

Ст. 158 УК РФ. Кража.

Предметом хищения в анализируемой статье является чужое имущество в виде денежных средств. При краже денежные средства изымаются безвозмездно, то есть без соответствующего возмещения.

Родовым **объектом** кражи денежных средств в системе ДБО являются общественные отношения в сфере экономики. Видовой и непосредственный объект: общественные отношения по охране собственности.

Характеризуя **объективные признаки** кражи денежных средств в системе ДБО, мы можем выделить общественно опасные действия и наступившие в их результате общественно опасные последствия. Общественно опасные действия в данном случае выражены активной формой поведения – действиями, направленными на тайное хищение чужого имущества в виде денежных средств. Общественно опасные последствия выражаются в нанесении материального ущерба потерпевшему.

Субъектом кражи является физическое вменяемое лицо, достигшее 14-летнего возраста, способное нести уголовную ответственность.

Субъективная сторона преступления в виде кражи денежных средств в системе ДБО характеризуется умышленной формой вины, прямым умыслом, корыстным мотивом.

Цель совершения преступления – материальное обогащение.

Согласно п. 6 постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. «О судебной практике по делам о краже, грабеже и разбое», кража считается оконченным преступлением с того момента, когда виновный изъяс чужое имущество и получил реальную возможность использовать его или иным образом распорядиться им по своему усмотрению¹⁰.

К **квалифицированным признакам** кражи денежных средств в системе ДБО следует отнести кражу, совершенную группой лиц по предварительному сговору (п. «а» ч. 2 ст. 158 УК РФ), с причинением значительного ущерба гражданину (п. «в» ч. 2 ст. 158 УК РФ).

¹⁰ Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. «О судебной практике по делам о краже, грабеже и разбое».

Кража признается совершенной группой лиц по предварительному сговору, если в ней принимали непосредственное участие два или более лица, заранее договорившиеся о совместном совершении кражи до начала преступления. При этом каждый из исполнителей либо полностью, либо частично выполнял объективную сторону преступления.

Кражу с причинением значительного ущерба гражданину следует квалифицировать в случае, если похищенные в системе ДБО денежные средства, принадлежавшие физическому лицу, существенно ухудшили его материальное положение. При этом ущерб не может признаваться значительным, если он составляет менее 5 000 рублей, согласно примечанию 2 к ст. 158 УК РФ.

Особо квалифицированные виды кражи денежных средств в системе ДБО предусмотрены п. «в» ч. 3 ст. 158 УК РФ – кража, совершенная в крупном размере; п. «г» ч. 3 ст. 158 УК РФ – с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ).

Крупный размер кражи в данном случае означает, что похищены денежные средства в размере, превышающем 250 тысяч рублей (примечание 4 к ст. 158 УК РФ).

Наиболее опасные виды кражи предусмотрены ч. 4 ст. 158 УК РФ: кража, совершенная организованной группой (п. «а») и в особо крупном размере (п. «б»). **Особо крупный размер** кражи означает хищение денежных средств в размере, превышающем 1 млн. рублей (примечание 4 к ст. 158 УК РФ).

Ст. 159.6 УК РФ. Мошенничество в сфере компьютерной информации.

Предметом рассматриваемого преступления в анализируемой статье является чужое имущество в виде денежных средств, похищенное путем обмана или злоупотребления доверием.

Родовым **объектом** в данном случае являются общественные отношения в сфере экономики. Видовой и непосредственный объект – общественные отношения по охране собственности.

Характеризуя **объективные признаки** хищения денежных средств в системе ДБО, совершенные путем обмана или злоупотребления доверием, мы можем выделить общественно опасные действия и наступившие в их результате общественно опасные последствия.

Общественно опасные действия в данном случае могут быть выражены активным обманом владельца денежных средств посредством сообщения ему заведомо ложных сведений, создающих у него ошибочное представление о совершаемых действиях. Такой обман может состоять в том, что преступник выдает себя, например, за сотрудника банка, тем самым создает иллюзию наличия законных оснований для сообщения ему

конфиденциальных сведений, необходимых для получения доступа к его денежным средствам.

Общественно опасные последствия выражаются в нанесении материального ущерба потерпевшему.

Субъектом мошенничества является физическое вменяемое лицо, достигшее 16-летнего возраста, способное нести уголовную ответственность.

Субъективная сторона преступления в виде хищения денежных средств в системе ДБО, совершенного путем обмана или злоупотребления доверием, характеризуется умышленной формой вины, прямым умыслом, корыстным мотивом.

Цель совершения преступления – материальное обогащение.

Специфика мошенничества состоит в том, что собственник имущества, введенный в заблуждение, может сам передавать преступнику свое имущество либо сообщать ему информацию, дающую право доступа к нему. При этом потерпевший ошибочно полагает, что действует в своих интересах.

Согласно п. 8 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество, то есть хищение чужого имущества, совершенное путем обмана или злоупотребления доверием, признается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц, и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распорядиться им по своему усмотрению.

Если предметом преступления при мошенничестве являются безличные денежные средства, в том числе электронные денежные средства, то по смыслу положений п. 1 примечаний к ст. 158 УК РФ и ст. 128 ГК РФ содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб¹¹.

На основании п. 20 вышеуказанного Постановления Пленума Верховного суда, по смыслу ст. 159.6 УК РФ вмешательством в функционирование средств обработки, хранения, систематизации и передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим

¹¹ Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, систематизации и передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 и 274.1 УК РФ¹².

К **квалифицированным признакам** преступления в виде хищения денежных средств в системе ДБО, совершенного путем обмана или злоупотребления доверием, следует отнести мошенничество, совершенное группой лиц по предварительному сговору, а также с причинением значительного ущерба гражданину (ч. 2 ст. 159.6 УК РФ).

Особо квалифицированные признаки анализируемого преступления предусмотрены ч.3 ст.159.6 УК РФ: деяния, совершенные лицом с использованием своего служебного положения (п. «а»); в крупном размере (п. «б»); с банковского счета, а равно в отношении электронных денежных средств (п. «в»).

Наиболее опасные виды мошенничества предусмотрены п. 4 ст. 159.6 УК РФ: деяния, совершенные организованной группой либо в особо крупном размере.

В целях квалификации преступлений по данной статье признаки понятия крупного и особо крупного размера похищенных денежных средств совпадают с признаками, используемыми при квалификации преступлений по ст. 158 УК РФ (см. примечание 4 к ст. 158 УК РФ).

Итак, выше нами были проанализированы элементы составов преступлений в системе ДБО, предусмотренных ст. 158 и ст. 159.6 УК РФ, выявлены квалифицирующие и особо квалифицирующие признаки по данным составам, приведены понятия оконченного преступления, крупного и особо крупного размера, применяемых в целях квалификации по вышеуказанным статьям.

С целью проведения анализа криминалистической информации, характеризующей особенности преступлений в системе ДБО, необходимо установить **место, время, способ, обстоятельства** совершения преступления, используемые **технические средства**, выявить **следы** приготовления, совершения преступления, а также их возможное сокрытие.

Временем совершения преступления в системе ДБО следует признавать момент нажатия управляющей клавиши компьютера (или другого

¹² Там же.

устройства), запускающей конечную целевую команду. При этом, в зависимости от способа совершения преступления, общественно опасные последствия могут наступить сразу после его совершения либо через длительное время, которое может потребоваться для действия используемой вредоносной программы.

Что касается определения места совершения преступлений, то в большинстве случаев – это компьютерные и (или) телекоммуникационные сети. Местом преступления может признаваться как место совершения общественно опасного деяния, так и место наступления общественно опасных последствий, при этом они могут быть отделены друг от друга многими километрами и даже континентами.

К способам преступлений, совершаемых в системе ДБО, относятся: использование вредоносных программ скрытого управления, использование программ считывания пароля, применение программ удаленного доступа, создание «зеркального сайта» и другие.

Анализу подлежат также все обстоятельства, сложившиеся в момент совершения преступления. Они влияют на выбор способа, механизма совершения преступления, позволяют определить причины и особенности поведения участников общественно опасного деяния.

К используемым техническим средствам относятся банкоматы, терминалы, компьютеры, планшеты, телефоны, платежные карты (финансовые инструменты), специальные устройства считывания и копирования информации с платежной карты, терминала или банкомата, другие технические средства и оконечные устройства.

Следами, позволяющими установить лицо, совершившее преступление, являются: сведения об IP-адресах, сведения о запросах к интернет-сайтам, следы подбора паролей, программы для удаленного администрирования, вредоносные программы, сведения о загрузке и выгрузке файлов, переписка, звонки, геолокационные данные мобильных устройств, информация из социальных сетей и др.

Проанализировав элементы, составляющие криминалистическую характеристику преступлений, совершенных в системе ДБО, мы можем сделать вывод о том, что в ходе расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, наибольшей спецификой обладают электронные следы преступлений. Они представляют собой результаты создания, преобразования компьютерной информации в форме копирования, изменения, модификации, блокирования, уничтожения, непосредственно связанных с совершением преступления. Именно такие электронные следы подлежат тщательному всестороннему исследованию.

Предположим, что если со счета клиента банка были похищены денежные средства без ведома его владельца, то данное преступное деяние, согласно нормам ст. 158 УК РФ, можно квалифицировать как **кражу**. Что же касается преступления в виде **мошенничества**, совершаемого в сфере компьютерной информации и телекоммуникационной сети, то в данном случае должны присутствовать: корыстная цель со стороны участника преступления или же соучастника, обман и злоупотребление доверием клиента, сопряженные с вводом, последующим удалением, блокированием, модификацией имеющейся и хранящейся в технических средствах информации. В этом случае такое противоправное деяние будет квалифицироваться как **мошенничество** по ст. 159.6 УК РФ.

Согласно нормам ст. 160 УК РФ «**Присвоение или растрата**», в действиях злоумышленника должно присутствовать противоправное безвозмездное обращение денежных средств в свою пользу или пользу других лиц с использованием ДБО сотрудником (работником), которому доверено в силу его должностного или иного служебного положения иметь доступ к лицевому счету клиента.

В п. 12 постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2007 года № 51 дается разъяснение, что основываясь на положениях ст. 140 ГК РФ, мошенничество считается оконченным с того момента, когда лицо перечислило денежные средства на банковский счет виновного либо на счета других лиц.

Ст. 160 УК РФ. Присвоение или растрата.

Присвоение и растрата – два вида противоправных деяний, имеющих один и тот же объединяющий признак: **похищение материальных ценностей**, которые обвиняемый или подозреваемый получил во временное распоряжение.

Обращение преступником материальных ценностей, принадлежащих иному лицу или государству, в личную собственность квалифицируется как присвоение. Лицо, владеющее ими, передает материальные ценности преступнику не навсегда, а во временное пользование. Это выражается в отсутствии действий по их отчуждению.

Присвоение и растрату денежных средств возможно рассматривать применимо и к сфере ДБО. По мнению авторского коллектива, преступления в сфере дистанционного банковского обслуживания подразумевают хищение денежных средств с банковских счетов клиентов сотрудниками банков, которые в силу своих должностных обязанностей имеют возможность доступа к денежным средствам клиентов, последующего присвоения и их растраты.

Преступное деяние, совершаемое в личных целях, квалифицируется как растрата. Ее сутью является передача чужих материальных ценностей

в расходование, пользование или потребление иным лицам с нарушением действующих правовых норм. Материальные ценности, а именно денежные средства в данном случае вверяются лицу, совершившему противоправное деяние в соответствии с договором на оказание банковских услуг.

Присвоение и растрата в сфере дистанционного банковского обслуживания может совершаться только в виде незаконных действий, направленных на хищение денежных средств в виртуальном пространстве.

Основопологающим признаком растраты и присвоения считается то, что собственник денежных средств не давал своего согласия на их отчуждение.

Для данного вида преступных деяний предусмотрен специальный субъект – дееспособное, 18-летнее лицо, сотрудник (работник) банка, имеющий в силу своих должностных полномочий доступ к лицевому счету клиента банка.

Если в присвоении и растрате участвовало несколько человек, их следует считать **пособниками, подстрекателями или организаторами.**

В ходе судебного разбирательства должно быть установлено, что лицо, совершившее противоправные деяния, имело корысть и умысел. Основным признаком корысти является желание преступника использовать чужие имущественные ценности в личных интересах.

Считаем необходимым рассмотреть **основные различия между растратой и присвоением.** Эти два вида квалифицируются по одной статье Уголовного кодекса Российской Федерации, но имеют **ряд различий.**

Под присвоением принято понимать противоправный переход права собственности к лицу, ранее не являющемуся его собственником. Ценность похищенного не уменьшается и его без ущерба можно возвратить законному собственнику.

При растрате нередки случаи, когда возврат похищенного невозможен. Поэтому у лица, совершившего растрату, возникает ответственность по возмещению нанесенного ущерба.

Присвоение считается завершенным, когда **начались действия по переходу права собственности к лицу, совершающему это противоправное деяние.** Завершением растраты считается момент, когда произошло **отчуждение ценностей**, вверенных лицу, совершающему противоправное деяние.

Нормы ст. 160 УК РФ имеют отличия от иных статей Уголовного кодекса, сходных ей по составу.

Схожими по составу с этой статьей в Уголовном кодексе Российской Федерации являются ст. 158 «Кража» и ст. 159 «Мошенничество». Однако для правильной квалификации именно растраты или присвоения необходимо знать основные признаки схожих между собой преступлений.

Основным признаком, характеризующим кражу, является тайность осуществляемого деяния, которое совершается без очевидцев или в том случае, когда вор уверен в этом. **Основным отличием кражи от растраты или присвоения является то, что преступник до совершения преступления не владел похищенными ценностями.**

Основным признаком мошенничества является перевод материальных ценностей, принадлежащих жертве, в пользу иного лица при помощи психологического воздействия на нее.

Если при растрате или присвоении собственник материальных ценностей на добровольной основе передает их на хранение или в пользование, то при мошенничестве или краже этот признак отсутствует.

Квалифицирующие признаки присвоения и растраты сформулированы в ч. 2, 3 и 4 ст. 160 УК РФ. Квалифицированным видом вышеупомянутых преступных деяний является осуществление присвоения или растраты группой лиц по предварительному сговору (**ч. 2 ст. 160 УК РФ**). Категория «**группа лиц по предварительному сговору**» определяется в ч. 2 ст. 35 УК РФ. Сравнительный анализ ч. 2 и ч. 1 ст. 135 УК РФ позволяет сформулировать вывод о том, что этот признак предполагает существование двух или более соучастников, которые заранее договорились о реализации преступного деяния, установленного ч. 2 ст. 160 УК РФ. Ввиду того, что группа лиц по предварительному сговору признается отдельной формой соучастия, осуществление хищения только одним гражданином при участии иных граждан, не соответствующих критериям субъекта преступления, не повлечет за собой возникновение рассматриваемого квалифицирующего признака ст. 160 УК РФ.

Присвоение или растрата, совершенные **с причинением значительного ущерба гражданину**, установлены в ч. 2 ст. 160 УК РФ. Согласно ч. 2 ст. 19 Конституции Российской Федерации в России гарантируется соблюдение принципа равенства прав и свобод человека и гражданина, причем независимо от того, какое имущественное положение занимает конкретный гражданин, в связи с чем при определении значительности ущерба стоит опираться на фактическую сумму присвоенных или растраченных средств со счета клиента банка.

Присвоение или растрата, реализованные гражданином с использованием своего служебного положения, раскрываются в ч. 3 ст. 160 УК РФ.

Следует отметить, что в случае присвоения и растраты, совершенных посредством ДБО, под данным лицом подразумевается сотрудник банка, имеющий доступ к персональным данным и счетам клиентов банка. Может быть ситуация, при которой денежные средства на счетах предоставляются не непосредственно виновному гражданину, а другим гражданам.

При этом ввиду занимаемого должностного положения гражданин обладает компетенцией по управлению и распоряжению через других граждан. Данные компетенции применяются виновным гражданином вопреки интересам службы для неправомерного завладения денежными средствами или передачи их с корыстной целью другим гражданам. Безусловно, служебное положение преступника характеризуется тем видом деятельности и набором компетенций, которые им реализуются. Соответственно, гражданин, реализующий служебную деятельность, бесспорно, занимает конкретное служебное положение. Значит, такое положение может им применяться при реализации преступного деяния, установленного ч. 3 ст. 160 УК РФ. Стоит отметить, что в правоприменительной практике реализация служебной деятельности трактуется как действия гражданина, включенные в перечень его профессиональных обязанностей, установленных конкретным трудовым договором или служебным контрактом, заключенным с организацией, государственным или муниципальным учреждением, а также предпринимателями, осуществление деятельности которых согласуется с действующими законодательными требованиями. **Крупным размером присвоения или растраты** (ч. 3 ст. 160 УК РФ) признается стоимость имущества, превышающая 250 тыс. руб. Данное положение указано в примечании 4 к ст. 158 УК РФ. Присвоение или растрата, реализованные организованной группой, раскрывается в ч. 4 ст. 160 УК РФ. **Главной особенностью**, позволяющей отграничивать организованную группу от группы лиц по предварительному сговору, следует считать **устойчивый характер**. Высокий уровень опасности преступного деяния, реализованного организованной группой, характеризуется и иными факторами. Однако данные признаки не имеют свойства перманентности, или их невозможно формализовать. В случае признания хищений реализованными организованной группой поведение всех соучастников должно быть квалифицировано как соисполнительство без указания ст. 33 УК РФ. При этом личный вклад в совершение преступного деяния, установленного ст. 160 УК РФ, никакого юридического значения не имеет. В правоприменительной деятельности судебные органы, как правило, констатируют устойчивый характер группы в том случае, если доказана продолжительность реализации противоправной деятельности. Руководители организованных групп привлекаются к уголовной ответственности за все реализованные такой группой преступные деяния, установленные ст. 160 УК РФ, если они охватывались их умыслом. Особо крупным размером присвоения или растраты (ч. 4 ст. 160 УК РФ) признается стоимость имущества, превышающая 1 млн. руб. Это следует из содержания примечания 4 к ст. 158 УК РФ.

Для того, чтобы определить **криминалистическую характеристику** данного преступления необходимо верно определить его вид и группу.

Присвоение и растрата является преступлением в сфере экономики и направлено против собственности, совершается дистанционно с использованием вверенных личных данных клиента банка. **Механизм** данного преступления заключается в безвозмездном обращении денежных средств в свою пользу или в пользу других лиц с использованием ДБО. Личность преступника соответствует вышеупомянутому специальному субъекту. **Предметом доказывания** в случае присвоения и растраты посредством ДБО будет:

- наличие информации о проделанном виртуальном пути похищенных денежных средств со счета клиента банка на счет преступника;
- данные, подтверждающие проведение определенных банковских операций конкретным виновным лицом.

Необходимым условием для начала уголовного преследования по ст. 160 УК РФ «Присвоение или растрата» является наличие следующих факторов:

- объект преступных деяний;
- имущественные ценности;
- мотив;
- умысел;
- состав преступных деяний в виде материальных ценностей.

При отсутствии любого из перечисленных признаков начать уголовное преследование по ст.160 УК РФ невозможно.

Квалификация тяжести преступления производится на основании установления стоимости растраченных или присвоенных материальных ценностей. Для этого при необходимости назначается дополнительная экспертиза. При определении статьи, по которой квалифицируются эти преступные деяния, судом учитывается состояние жертвы и значимость материальных ценностей для нее, таких как источники дохода и стоимость присвоенных или растраченных ценностей; наличие несовершеннолетних детей, родителей пожилого возраста и иных иждивенцев; общий размер получаемых всеми членами семьи доходов; мнение жертвы о значимости нанесенного ущерба.

Согласно постановлению Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» указано, что такие преступные деяния, как растрата и присвоение относятся к категории преступлений, имеющих экономический характер. Конечной целью таких преступных деяний является присвоение и использование чужих материальных ценностей для получения личной выгоды.

Правовые нормы действующего Уголовного Кодекса Российской Федерации за растрату или присвоение указывают, что, исходя из ситуа-

ции, могут назначаться как штрафы соответствующего размера, так и принудительная изоляция на различные сроки.

Об этом красноречиво говорит следующий конкретный пример, выявленный сотрудниками ПСТМ МВД России:

Пример.

В Республике Дагестан сотрудник-бухгалтер органов внутренних дел задержана по подозрению в мошенничестве и растрате.

Будучи наделённой правом подписи и имея доступ к банковскому счёту отдела полиции города Каспийска, женщина внесла недостоверные сведения в заявке на кассовый расход и направила их для исполнения. На основании этих документов на её банковский счёт и счёт её подруги казначейством республики были перечислены денежные средства в сумме около 570 тысяч рублей, которыми правонарушительница распорядилась по своему усмотрению.

В отношении неё возбуждено уголовное дело по ст. 159 ч. 3, ст. 160 ч. 3 УК РФ, проводятся мероприятия, направленные на закрепление доказательной базы.

Подводя итог проведенной уголовно-правовой и криминалистической характеристики ст. 158, 159 и 160 УК РФ в сфере дистанционного банковского обслуживания можно сделать вывод о том, что данный вид преступлений является последствием развития банковских технологий. Реализация информационных, документационных, компьютерных технологических инноваций обеспечивает оптимизацию рабочего процесса в сфере обслуживания клиентов банками. Однако такие возможности могут являться благоприятным условием для совершения противоправных деяний в отношении граждан, предоставляющих банкам свои персональные данные и денежные средства на хранение.

В связи с вышеизложенным сотрудникам правоохранительных органов требуется постоянное повышение профессиональной квалификации в области современных технологий банковского обслуживания, в том числе и международного уровня. Кроме того, необходимо разработать методику своевременного предупреждения, выявления, раскрытия и расследования данного вида преступлений и внедрить в практическую деятельность сотрудников органов внутренних дел.

Анализируя практический опыт раскрытия преступлений в системе ДБО сотрудниками органов внутренних дел, необходимо отметить, что одним из основных элементов криминалистической характеристики преступлений является способ совершения преступления.

4.2. Некоторые способы хищения денежных средств в системе дистанционного банковского обслуживания

Предлагаем рассмотреть некоторые способы преступлений, совершаемых в системе ДБО¹³:

- использование вредоносных программ скрытого управления;
- использование программ считывания пароля;
- применение программ удаленного доступа;
- создание «зеркального сайта»;
- перечисление денежных средств преступниками на «электронные кошельки»;
- ложная информация «проблема у родственника»;
- получение звонков, SMS-сообщений «Ваша карта заблокирована»;
- размещение объявления на сайте «Авито» и иных ресурсах сети Интернет;
- «Мобильный банк»;
- заражение вредоносным программным обеспечением телефонных аппаратов и других технических устройств на операционной системе «Android».

Использование вредоносных программ скрытого управления

В данном случае преступниками используется вредоносная программа, которая проникает и устанавливается в мобильный телефон потерпевшего. Далее она *самостоятельно* (без непосредственных команд преступников) рассылает с него SMS-сообщения, управляя его банковским счетом через услугу «Мобильный банк».

Данная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в SMS или MMS-сообщениях. Кроме того, потерпевшие сами неосознанно могут устанавливать на мобильные устройства вредоносные программы, замаскированные под игры и другие программные продукты.

Одним из признаков (необязательным) наличия вредоносной программы на мобильном телефоне является направление «пустых» SMS или MMS-сообщений на телефоны, имеющиеся в контактах устройства. При открытии адресатом такого SMS или MMS происходит дальнейшее заражение вирусом телефонов, получивших данное сообщение.

Возможно получение потерпевшим в виде SMS с номера 900 или других сервисных номеров различной информации, которую он не запрашивал. Это связано с тем, что направление информации с сервисных номеров вызвано действиями вредоносных программ.

¹³ Данный перечень не является исчерпывающим, так как возможно появление новых способов хищений денежных средств, а также в какой-то части измененных.

Одним из способов первичного средства выявления вредоносных программ на телефоне является использование антивирусных программ, получение детализации телефонных звонков и SMS. При наличии вредоносной программы в разделе детализации «исходящие SMS» будут сообщения, которые владелец телефона не направлял на сервисный номер 900 либо номера, используемые преступниками для списания средств потерпевшего через поступившие SMS.

Пример 1.

Сотрудниками БСТМ МВД России в рамках оперативного сопровождения уголовного дела, возбужденного СЧ ГУ МВД России по СФО по ч. 2 ст. 273 УК РФ, установлены и задержаны участники организованной преступной группы, действовавшей под руководством жителя г. Владикавказа, который разработал уникальное вредоносное программное обеспечение для хищения конфиденциальной информации и скрытой генерации криптовалюты на «зараженных» технических устройствах.

Следственные действия в отношении участников группы по множеству фактов противоправной деятельности производились одновременно на территории 9 субъектов Российской Федерации.

Данный пример красноречиво говорит о причиненном вреде клиентам банков в особо крупном размере и его территориальной масштабности.

Пример 2.

В результате сопровождения уголовного дела, возбужденного по ч. 4 ст. 159 УК РФ, сотрудниками БСТМ МВД России на территории г. Москвы установлен и задержан злоумышленник, которым разработано уникальное программное обеспечение, позволяющее эксплуатировать уязвимости терминалов системы «UPOS» и получать одобрение платежных операций без подтверждения банком. Указанной уязвимости на текущий момент времени оказалось подвержено более 1,7 млн. платежных терминалов ПАО «Сбербанк России».

Пример 3.

В ходе раскрытия преступления было установлено, что мошенники расклеивали QR-коды на прокат автомобилей и велосипедов, где не было продавцов. Клиент, ничего не подозревая, сканировал QR-код, после чего оплачивал услуги по прокату. Но денежные средства поступали напрямую мошенникам на их лицевые счета, и клиент оставался без денежных средств и услуг проката (см. рис. 3).



Рис. 3. Мошенничество с использованием QR-кода

Использование программ считывания пароля

В этом случае в индивидуальное электронное устройство потерпевшего проникает и устанавливается вредоносная программа, которая фиксирует вводимый пользователем логин и пароль в момент доступа к удаленному банковскому сервису (например, «Сбербанк Онлайн»). Преступники позже, используя этот логин и пароль, входят в личный кабинет пользователя с другого компьютера и совершают хищение.

Применение программ удаленного доступа

Преступниками используется программа, которая предварительно устанавливается на электронное устройство потерпевшего лица. Она позволяет в режиме реального времени отправлять на него команды управления через сеть Интернет (действие аналогично программе «Android» и др.). Отличие от способа, рассмотренного выше, заключается в непосредственном управлении преступниками перечислением похищаемых денежных средств путем удаленного направления команд мобильному устройству (данный способ встречается сравнительно реже иных).

Рассмотрим пример, взятый из практической деятельности БСТМ МВД России, носящий межрегиональный характер.

В ходе оперативного сопровождения уголовного дела, возбужденного СО СУ УМВД по ВАО ГУ МВД России по г. Москве по ч. 4 ст. 159.6 УК РФ, установлены и задержаны уроженцы Саратовской области и их соучастники, которые совершали хищения денежных средств посредством

несанкционированного подключения к банкоматам различных кредитно-финансовых учреждений. Общий ущерб от противоправной деятельности фигурантов на территории более 15-ти субъектов Российской Федерации превысил 30 млн. рублей.

Благодаря оплаженным действиям сотрудников БСТМ МВД России по организации межрегионального взаимодействия в ходе проведения оперативно-розыскных и иных необходимых мероприятий важную роль сыграло своевременное получение криминалистически оперативно значимой информации. Тактически грамотное планирование оперативного сопровождения уголовного дела способствовало своевременному обнаружению и анализу информации обо всех совершенных преступлениях рассматриваемого вида и установлению лиц, причастных к ним.

Создание «зеркального» сайта

Данный способ возможен, когда потерпевший пользуется «личным кабинетом» на сайте банка. Преступниками создается и используется фейковый (поддельный) сайт, адрес которого и внешнее оформление страниц трудноотличимы от официального сайта банка, интернет-магазинов, страницы в социальных сетях. Если потерпевший при входе на сайт банка не использует сохраненную ссылку, а просто набирает название банка в поисковой системе, то ему обычно предлагается несколько вариантов. Если потерпевшим будет осуществлен вход на «зеркальный» сайт, то вводимыми данными для входа в кабинет банка (логин и пароль) могут воспользоваться злоумышленники и войти на настоящем сайте от имени потерпевшего в его личный кабинет. Далее возможен перевод денег со счета потерпевшего из личного кабинета или подключение к его счету услуги «мобильный банк» на любом абонентском номере.

Основным признаком посещения клиентом «зеркального» сайта банка является то, что после ввода логина и пароля на странице пользователя появляется надпись о техническом обслуживании сайта или любая иная информация. В данном случае **информационное SMS-сообщение** от банка о входе в личный кабинет **может отсутствовать** или поступит информация, в которой будет указано: **«Обратиться на сайт позднее»**. Данное обстоятельство создает благоприятные условия и временной период злоумышленнику для хищения денежных средств со счета лица, которое само предоставило все сведения о наличии денежных средств.

Одним из главных признаков преступлений в сфере информационных технологий является то, что совершать преступления могут лица вне зависимости от возраста и полученного образования.

Преступления в сфере компьютерной информации совершаются **преимущественно молодыми людьми**, ранее не привлекавшимися к уголовной ответственности. Наибольшую криминальную активность прояв-

ляют лица от 14 до 35 лет. Значительная их часть имеет специальное образование, связанное со сферой компьютерных технологий, но встречаются и те, кто получил знания и навыки, способствующие совершению преступлений, самостоятельно.

Их положение в обществе может варьироваться от школьника и студента до ответственного сотрудника учреждения, компании (фирмы). Вместе с тем данный вид преступлений могут совершать и высококвалифицированные специалисты, владеющие полной информацией и способные создавать вредоносные программы и знать их принцип работы.

Отдельные члены преступной группы в некоторых случаях могут проживать в различных регионах и до момента задержания и доставления в органы внутренних дел лично не встречаться с другими соучастниками. Для знакомства и координации своих действий они используют сайты и специальные сетевые ресурсы, где обсуждают способы совершения преступлений и маскировки следов.

Перечисление денежных средств преступниками на «электронные кошельки»

Преступники при совершении преступлений в сфере информационных технологий часто используют «электронные кошельки» платежных систем Yota, RBK-money, Yandex-деньги и подобные им. Предпочтение злоумышленников использованию «электронных кошельков» объясняется тем, что последние выполняют функции банковского счета, не требуя ни указания персональных данных его владельца (как правило, указываются вымышленные данные), ни его непосредственной идентификации при проведении финансовых операций. Зарегистрировать «электронный кошелек» можно через сеть Интернет, при этом указав вымышленное имя, либо вообще вместо имени ввести случайное сочетание букв и цифр. Преступниками «электронные кошельки» в основном используются как «промежуточное звено» в цепи перемещения похищенных денежных средств. После поступления на используемые злоумышленниками «электронные кошельки» денежные средства далее переводятся на другие «электронные кошельки», счета номеров сотовой связи или банковские счета.

Для выявления лиц, совершивших хищения, сотрудникам органов внутренних дел в этом случае необходимо устанавливать «IP-адреса» технических устройств, с которых регистрировался «электронный кошелек» и осуществлялся выход в сеть при совершении платежной операции, а также **отслеживать путь** перечисления денежных средств с «электронного кошелька» (на какие другие «электронные кошельки» или счета) **путем запроса в администрацию электронной платежной системы**. При этом целесообразно ставить вопрос не только о счетах, на которые перечислялись средства, но и об иных счетах, с которых совершалось перечисление на выявленный «электронный кошелек» (для установления других потерпевших и «электронных кошельков», используемых преступниками).

Ложная информация «проблема у родственника»

Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) возникла проблема (попал в ДТП, совершил преступление, иное) и предлагает ему разрешить эту проблему, но при этом необходимо заплатить определенную денежную сумму. Потерпевший соглашается и ждет человека, которому необходимо передать деньги.

Преступник звонит в такси и через оператора узнает номер таксиста. Таксисту преступник сообщает, что ему необходимо подъехать к условленному адресу, где ему передадут деньги. Прибыв по указанному адресу, таксист получает определенную денежную сумму и информирует об этом преступника.

Злоумышленник сообщает таксисту номера телефонов, на которые необходимо перевести денежные средства, полученные от потерпевшего. С помощью банкомата (терминала) таксист осуществляет перевод денежных средств на номера телефонов, указанные ему преступником (телефонных номеров может быть несколько).

При поступлении денежных средств на различные номера телефонов осуществляется их перевод на единый расчетный счет банка (пластиковой карты). Соучастник преступления, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или Интернет), переводит денежные средства преступнику.

Для данной схемы часто случается упрощенная вариация, при которой исключаются действия с таксистом, при этом платежные операции производятся потерпевшим самостоятельно (схема аналогична случаю с сообщениями о блокировке банковских карт):

- преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) возникла проблема (попал в ДТП, совершил преступление, иное) и предлагает ему разрешить данную проблему, но при этом необходимо заплатить определенную денежную сумму. Потерпевший соглашается, и преступник указывает ему номера телефонов, банковских карт и т.п., на которые необходимо зачислить денежную сумму;

- потерпевший с помощью банкомата (терминала) осуществляет перевод денежных средств на номера телефонов, указанные ему преступником. При этом возможно будет указано несколько телефонных номеров.

При поступлении денежных средств на различные номера телефонов, осуществляется их перевод на указанный расчетный счет банка (пластиковой карты). Далее соучастник преступления, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или Интернет) переводит денежные средства преступнику (см. рис. 4).

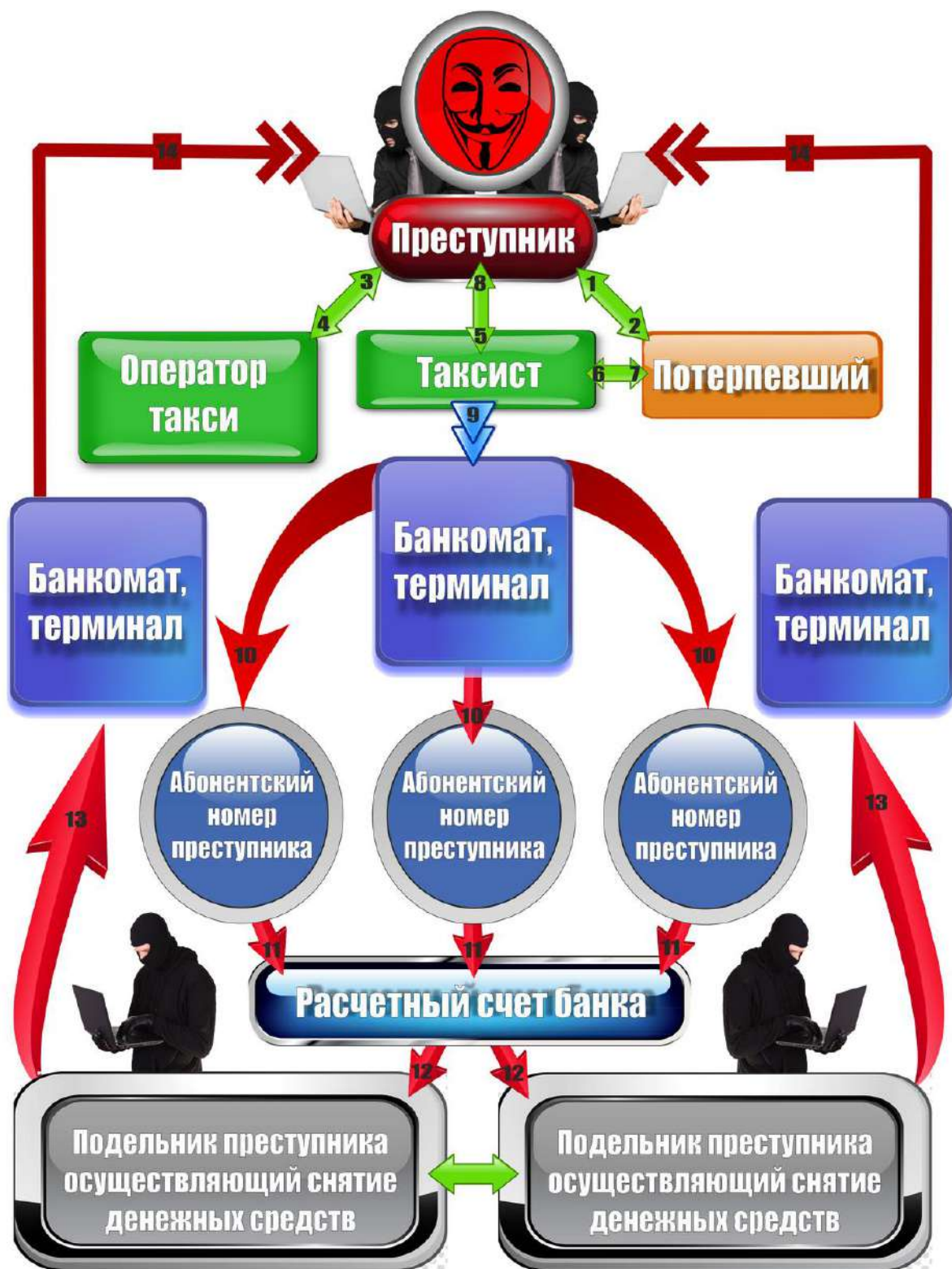


Рис. 4. Общая схема преступной деятельности «проблема у родственника»



Рис. 5. Пример успешного взаимодействия

Предлагаем рассмотреть следующий пример.

Мошенники приобретали базы данных с персональными сведениями граждан Московского региона и осуществляли звонки на сотовые и стационарные телефоны жителей Московского региона, представляясь сотрудниками службы социального обеспечения (Собес) и предлагали получить компенсацию за неиспользованные путевки в г. Геленджик.

Благодаря тесному взаимодействию службы кибербезопасности ПАО «Сбербанк» и сотрудников органов внутренних дел Российской Федерации все члены организованной преступной группы были изобличены и понесли соответствующие наказания (см. рис. 5).

В случаях совершения хищений денежных средств со счетов клиентов банков и получения информации о подготавливаемом или совершенном преступлении необходимо применять предлагаемый алгоритм действий:

1. Подробно опросить потерпевшего об обстоятельствах происшествия. С целью установления абонентского номера злоумышленника необходимо от потерпевшего получить заявление на предоставление сведений о соединениях в момент совершения преступления.

2. Прибыть на место происшествия, где потерпевший передавал денежные средства. Определить границы осмотра, произвести качественный осмотр места происшествия с привлечением эксперта (специалиста) для своевременного обнаружения и последующего изъятия возможных характерных следов данного вида преступления с целью дальнейшей идентификации лица, получившего от потерпевшего деньги.

3. Установить очевидцев и свидетелей. С этой целью произвести поквартирный (подомовой) опрос граждан для получения информации о лице, которому были переданы денежные средства, и наличии автотранспорта. Составить словесный (композиционный) портрет подозреваемого лица.

4. Установить наличие видеокамер (видеодомофонов), видеорегистраторов, фиксирующих различного рода действия в зоне совершения преступления.

5. Осуществить выборку автомобилей по полученной информации о части буквенной или цифровой серии госномерного знака автотранспортного средства, на котором передвигался злоумышленник (подозреваемое лицо), и проверить их собственников на осуществление ими частного извоза в составе таксомоторной компании.

6. Направить запросы в таксомоторные компании о выезде таксистов, работающих у них в компании, на адрес, где осуществлялась передача денежных средств.

7. При определении госномерных знаков, принадлежащих автомобилю, установить лицо, которому потерпевший передал денежные средства. При установлении лица, которому потерпевший передал денежные средства (водитель такси), опросить его. *В ходе опроса необходимо установить следующее:*

- кому и каким способом передавались денежные средства, полученные от потерпевшего;
- каким способом осуществлялась связь с лицом, которое сообщило ему, куда и как перевести денежные средства, полученные от потерпевшего;
- подробное описание голоса лица, звонившего таксисту;
- установить номер телефона, с которого звонили таксисту;
- истребовать с таксиста и таксомоторной компании, в которой он работает, детализацию по используемому абонентскому номеру (входящие и исходящие соединения) за период поступления звонка преступника для последующего анализа.

8. В случае если таксист, по указанию злоумышленника, перевел денежные средства через терминал (банкомат) на абонентские номера, то необходимо установить номера, на которые были переведены денежные средства потерпевшего, и местонахождение терминала (банкомата).

9. Опросить оператора такси.

10. После проведения необходимых оперативно-розыскных мероприятий по выявлению обстоятельств и лиц, причастных к совершению преступления, принять неотложные меры для решения вопроса о возбуждении уголовного дела.

11. Направить запросы (судебные решения) операторам сотовой связи с целью установления:

- владельцев абонентских номеров, использованных для совершения преступления, и их местоположения в момент совершения преступления;
- IMEI телефонов, с которых звонил преступник;
- детализации с указанием информации об абонентах;
- движения денежных средств по счетам абонентских номеров, на которые были зачислены денежные средства потерпевшего, и абонентских номеров, с которых звонил преступник.

12. При получении ответов от операторов сотовых компаний необходимо осуществить анализ данной информации:

- установить наличие учреждения ФСИН России, находящегося рядом с местом, указанным в географическом положении абонентского номера, с которого звонил преступник в момент совершения преступления;
- проанализировать детализацию с целью установления лица, совершившего преступление;
- установить номер счета, на который были перечислены денежные средства, и установить дальнейшее движение денежных средств с этого номера. Если деньги обналичивались, то установить место (банкомат, отделение связи, интернет-ресурсы), где была совершена данная денежная

операция, и осуществить направление необходимых запросов в организации, осуществляющие денежные переводы для установления лица, осуществившего снятие денежных средств;

- при определении места расположения исправительного учреждения, откуда был осуществлен звонок, направить запрос с целью обнаружения и последующего изъятия сотрудниками ФСИН России телефонных аппаратов с указанными идентификационными номерами и SIM-карт.

13. Сотрудники, ответственные за формирование информационно-поисковой системы (ИПС), осуществляют ввод информации в базу данных и ее корректировку при получении новых сведений.

Получение звонков, SMS-сообщений «Ваша карта заблокирована»

Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего или отправляет ему SMS-сообщение о том, что «Ваша карта заблокирована» (или об иной проблеме со счетом, пластиковой картой). В процессе беседы злоумышленник предлагает потерпевшему для решения внезапно возникшей неблагоприятной ситуации осуществить в кратчайший срок ряд операций через ближайший банкомат. По прибытию к банкомату потерпевшее лицо созванивается с преступником и выполняет все его указания.



Рис. 6. Общая схема преступной деятельности «Ваша карта заблокирована»

Преступник сообщает потерпевшему набор цифр для устранения проблем с картой (счетом). При поступлении денежных средств на различные номера телефонов осуществляется их перевод на единый расчетный счет банка (пластиковой карты).

Сообщник преступления, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или Интернет), осуществляет перевод денежных средств преступнику (см. рис. 6).

В случаях осуществления преступной деятельности «Ваша карта заблокирована» необходимо применять следующий алгоритм действий:

1. Опросить потерпевшего и очевидцев.
2. Истребовать распечатку детализации соединений потерпевшего.
3. Установить, на какие номера (расчетные счета) потерпевший перевел денежные средства.
4. В случае если денежные средства были переведены на телефонные номера, необходимо направить запросы (судебные решения) операторам сотовой связи с целью установления:
 - владельцев сим-карт;
 - IMEI используемых злоумышленниками телефонов;
 - географического местоположения, детализации с указанием информации об абонентах;
 - движения денежных средств по счетам абонентских номеров, на которые было осуществлено зачисление денежных средств потерпевшего, и по абонентскому номеру, с которого звонил злоумышленник.
5. В случае если денежные средства были переведены на расчетные счета банковских карт, другие банковские счета, необходимо направить запрос в банк, в котором обслуживается клиент-потерпевший, с целью получения информации о расчетных счетах, использованных злоумышленником.
6. Принять решение о возбуждении уголовного дела.
7. Сотрудники, ответственные за формирование ИПС, осуществляют ввод информации в банк данных и ее корректировку при получении новых сведений.
8. В рамках возбужденного уголовного дела необходимо:
 - проанализировать детализацию с целью установления лица, совершившего преступление;
 - установить номер счета (абонентский номер), на который были перечислены денежные средства, и определить дальнейшее направление денежных средств с этого номера. В случае, если деньги обналичивались, то установить место (банкомат, отделение связи, интернет-ресурсы), где была совершена данная денежная операция, и направить необходимые запросы в организации, осуществляющие денежные переводы, для установления лица, снимавшего денежные средства;

- провести иные необходимые оперативные мероприятия и следственные действия, направленные на выяснение всех обстоятельств, причинно связанных с расследованием преступления, а также на установление лиц, причастных к совершению преступления.

Действия в ситуациях, когда предлогом мошенничества является выигрыш приза потерпевшим, оказание медицинских услуг и т.п., аналогичны вышеизложенным.

Размещение объявления на сайте «Авито» и иных ресурсах сети Интернет (потерпевший/преступник)

В среднем каждый день на сайте «Avito.ru» размещается около 2 500 объявлений.

В целях профилактики совершения мошенничеств с использованием интернет-ресурса «Avito.ru» уполномоченными сотрудниками ежедневно обзванивается в среднем 100 человек, что составляет 0,02% от общего числа объявлений и 2% – от поданных в текущий день.

Для повышения эффективности принимаемых мер и снижения числа мошенничеств, совершаемых в отношении пользователей сайта «Avito.ru», целесообразно привлекать к профилактической работе сотрудников следственно-оперативных групп территориальных органов внутренних дел.

Предлагаем рассмотреть пример, взятый из практической деятельности.

В отдел УМВД России по Кузнецкому району Пензенской области обратились граждане с заявлением о мошенничестве. Сотрудниками уголовного розыска отдела УМВД России по Кузнецкому району совместно с сотрудниками ПСТМ МВД России было выяснено, что потерпевший разместил на сайте «Avito.ru» объявление о продаже крупного рогатого скота. Злоумышленник воспользовался этим объявлением, чтобы создать свое «зеркальное» объявление на этом же сайте с указанием своего номера телефона.

Покупатели увидели «зеркальное» объявление и совершили звонок мошеннику. Мошенник позвонил настоящему продавцу и в процессе разговора, представившись потенциальным покупателем, выяснил необходимые подробности, такие как место нахождения товара, его окрас, вес, породу и размер, а также, где и когда можно посмотреть животных. Позже злоумышленник перезвонил настоящим покупателям и рассказал подробности про животный товар и его место расположения. Далее мошенник в разговоре сделал акцент на возможную скидку, если покупатели ускорят приобретение крупного рогатого скота. Покупатели были заинтересованы в покупке животных и намеревались приехать по обозначенному месту нахождения товара. Мошенник предупредил покупателей, что в момент просмотра животных он будет отсутствовать на ферме. Их встретит

его управляющий. При этом мошенник объяснил покупателям, что договариваться о стоимости с управляющим не нужно. В свою очередь, преступник настоящего продавца скота поставил в известность, что во время осмотра товара он будет находиться в Москве по причине своей занятости, и поэтому не сможет присутствовать на встрече. К продавцу придут работники «реального покупателя», и разговоры о стоимости животных с ними вести нет необходимости.

Согласно намеченному договору было проведено знакомство с товаром. Стороны договорились о конкретном времени предстоящей сделки купли-продажи. Мошенник, предвидя конечный результат, заранее подготовил настоящего продавца и настоящих покупателей о том, что им необходимо осуществить денежный перевод на указанный номер банковской карты.

В назначенное время настоящие покупатели совместно с настоящим продавцом отправились в ближайшее отделение «Сбербанка» и осуществили перевод денежных средств мошеннику на номер его банковской карты в размере 235 тыс. рублей.

После того, как транзакция состоялась, абонентский номер мошенника был выключен. Сотрудниками уголовного розыска отдела УМВД России по Кузнецкому району Пензенской области совместно с сотрудниками ПСТМ МВД России было установлено, что абонентский номер мошенника оформлен на гражданина ближнего зарубежья. Банковская карта, на номер которой осуществлялся перевод денежных средств, не имеет привязки к данным конкретного лица.

В настоящее время проводятся оперативно-розыскные мероприятия по установлению преступника.

Размещение объявления на сайте «Авито» и иных ресурсах сети Интернет (объявление разместил преступник)

Преступник размещает на сайте электронных объявлений («Авито» или иных сайтов) информацию о продаже каких-либо товаров, для связи указывает телефон. Потерпевший обнаруживает объявление и, решив приобрести заявленные в нем товары, созванивается с преступником по указанному в объявлении абонентскому номеру сотовой связи. Преступник сообщает лицу, что товар имеется в наличии, и злоумышленник готов его продать по низкой цене. В данном случае под разными предложениями преступник всегда отказывается показать товар, при этом сообщает, что интересующий товар находится в другом городе (субъекте Российской Федерации). Злоумышленник предлагает будущей жертве внести предоплату. Преступник и потерпевший еще некоторое время ведут телефонные переговоры, в ходе которых оговариваются цена товара, способ оплаты и сроки поставки.

Потерпевший перечисляет денежные средства на указанный злоумышленником банковский счет (карту, электронный кошелек, абонентский номер). После осуществления всех намеченных операций преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т.п. и затем обналичивает собранные денежные средства либо сам, либо через своих сообщников.

Размещение объявления на сайте «Авито» и иных ресурсах сети Интернет (объявление разместил потерпевший)

Потерпевший размещает на сайте электронных объявлений («Авито» или иных сайтов) информацию о продаже каких-либо товаров и для связи указывает номер телефона. Преступник обнаруживает объявление и созванивается с потерпевшим по указанному в объявлении абонентскому номеру сотовой связи, сообщает, что он готов приобрести товар, но в настоящее время находится в другом регионе и предлагает внести предоплату.

Потерпевший в ходе телефонного разговора сообщает преступнику реквизиты банковской карты (полный номер карты, срок действия и имя держателя, указанные на лицевой стороне), а также одноразовый пароль, подтверждающий операции по перечислению денежных средств со счета банковской карты, поступивший ему в SMS-сообщении с сервисного номера «900».

Путем перевыпуска сим-карты настоящего владельца преступник посредством услуги дистанционного банковского обслуживания «Сбербанк Онлайн» получает доступ ко всем счетам, открытым на имя потерпевшего и осуществляет списание с них денежных средств на используемые карты, счета. Далее преступник либо его сообщники обналичивают собранные денежные средства.

В случаях осуществления преступной деятельности путем размещения объявлений на сайте «Авито» и иных ресурсах сети Интернет необходимо применять следующий алгоритм действий:

1. Принять от потерпевшего подробное объяснение, в котором необходимо отразить:

- дату и время обнаружения объявления, по возможности найти само объявление в сети Интернет и зафиксировать его номер, сделать снимок экрана либо попросить потерпевшего предоставить указанные сведения;
- если объявление уже отсутствует, то, как можно более подробно, описать его (текст, средства связи с продавцом, цена товара, дата размещения объявления);
- способы связи потерпевшего с преступником, порядок взаимодействия (связь по телефону), отразить номера телефонов;
- дату и время звонков, период разговоров;

- способ перечисления преступнику денежных средств, реквизиты банковского счета, карты; название платежной системы (РВК.money, Яндекс.Деньги и т.п.); дату и время перевода денежных средств.

2. Направить оператору электронных объявлений («Авито» или иных сайтов) запрос с целью установления:

- даты и времени размещения объявления;
- контактных данных, указанных и использованных автором объявления;
- IP-адресов, даты и времени доступа автора объявления к сайту при размещении объявления и иных сеансах доступа.

3. Если потерпевший общался с преступником по телефону, истребовать у него детализацию звонков за данный период, в которой должен быть отражен номер телефона преступника.

4. Провести ОРМ «Наведение справок» по абонентским номерам, на которые осуществлен перевод денежных средств. При необходимости в целях установления региона, к емкости которого относятся абонентские номера, а также персональных данных владельца можно использовать возможности справочных программ в сети Интернет.

5. Принять решение о возбуждении уголовного дела.

6. После того, как потерпевший укажет номер счета (оператора связи, платежную систему), на который им осуществлялись перечисления денежных средств, направить запрос в банк с целью установления:

- сведений о владельце банковской карты, счета (клиента электронной платежной системы, оператора связи);
- сведений о дальнейшем движении поступивших средств до момента обналичивания либо вывода их из системы;
- IP-адресов, даты и времени доступа пользователя к системе (для электронных платежных систем).

7. При получении запрашиваемых сведений от операторов электронных объявлений, платежных систем, банков, операторов сотовой связи проанализировать поступившие сведения:

- установлено ли место обналичивания средств потерпевшего;
- установлен ли оператор связи, посредством которого размещено объявление в сети Интернет, велась ли электронная переписка;
- установлено ли географическое положение абонентских номеров, посредством которых преступник взаимодействовал с потерпевшим.

8. Сотрудники, ответственные за формирование информационно-поисковой системы, осуществляют ввод информации в базу данных и ее корректировку при получении новых сведений.

«Мобильный банк». «Двойной Мобильный банк»

Потерпевшим при заключении договора указывается абонентский номер, который и подключается к «Мобильному банку». По различным причинам многие владельцы пластиковых карт банков перестают в дальнейшем пользоваться абонентскими номерами (потерял, переехал, сменил оператора и т.д.), в связи с чем оператор сотовой связи через 6 месяцев перевыпускает SIM-карту с данным абонентским номером и выставляет ее на продажу. Также возможна утеря SIM-карты и не отключение ее «мобильного банка».

Новый абонент, приобретая данную SIM-карту, начинает получать SMS о движении денежных средств по счёту потерпевшего (бывшего владельца SIM-карты). Вследствие чего образуется «двойной мобильный банк». Все транзакции, проводимые бывшим владельцем SIM-карты, становятся известными как потерпевшему, так и новому владельцу. Кроме того, новый владелец SIM-карты получает возможность управлять денежными средствами лицевого счета, к которому она подключена.

Заражение вредоносным программным обеспечением телефонных аппаратов и других технических устройств на операционной системе «Android»

Потерпевший получает SMS или MMS-сообщение от контент-провайдера либо от неизвестного посредством сети Интернет со ссылкой на информационный ресурс, перейдя по которой, абонент закачивает на телефон вредоносное программное обеспечение (далее ВПО).

Потерпевший получает SMS-сообщение от своего «знакомого», телефон которого уже заражен ВПО, при этом ВПО само направляет данное сообщение на номера, которые имеются в адресной книге потерпевшего. В данном сообщении также находится ссылка на информационный ресурс, перейдя по которой, абонент закачивает на телефон ВПО.

Потерпевшее лицо, находясь в сети Интернет, с помощью телефона получает по электронной почте либо через социальные сети ICQ сообщение, в котором находится ссылка на информационный ресурс, перейдя по которой абонент закачивает на телефон ВПО.

Также потерпевшее лицо, находясь в сети Интернет, может с помощью телефона, скачивать, например, программные продукты, музыку, фотографии, в которых находится ссылка на конкретный информационный ресурс, перейдя по которой, абонент закачивает на телефон ВПО.



Рис. 7. Общая схема преступной деятельности «хищения денежных средств с помощью мобильного вируса»

После заражения телефона «вирус» проверяет наличие подключенной услуги «Мобильный банк». Если услуга подключена, то вирус с помощью нее осуществляет перевод денежных средств с банковской карты потерпевшего на различные абонентские телефонные номера, электронные платежные системы (Киви-кошелек и др.), либо на лицевой счет абонентского телефонного номера потерпевшего и далее на электронные платежные системы, либо банковские карты преступника. При этом вирус блокирует (не выводит на дисплей телефона, а также удаляет их из телефона потерпевшего) информационные SMS-сообщения о произведенных транзакциях, которые поступают от банка (рис. 7).

В случаях осуществления преступной деятельности «заражение вредоносным программным обеспечением телефонных аппаратов и других технических устройств на операционной системе «Android» необходимо применять следующий алгоритм действий:

В ходе опроса заявителя в обязательном порядке выяснить, подключена ли услуга «Мобильный банк», а также установить модель телефона, используемого потерпевшим. Кроме того, выяснить, имеется ли у потерпевшего аккаунт системы Киви-кошелек, «привязанный» к абонентскому номеру, приходили ли потерпевшему подозрительные сообщения на телефон с различными ссылками. Далее у потерпевшего необходимо выяснить:

- обращался ли он в банк, если да, то каким образом;
- какой был получен ответ от сотрудника банка (в устном или письменном виде).

Часто при получении SMS о снятии денежных средств со счета, потерпевшие обращаются по телефону в банк. В процессе телефонного разговора оператор сообщает, куда были перечислены денежные средства, с какого номера телефона было отправлено SMS, и иногда сообщается абонентский номер, на счет которого перечислены денежные средства. В случае, если у потерпевшего имеется детализация звонков и SMS от оператора сотовой связи, а также выписка из лицевого счета, то необходимо данные документы (или копии) приобщить к материалам проверки. Если вышеперечисленных документов при обращении в полицию у потерпевшего нет, то *после принятия заявления необходимо незамедлительно вместе с потерпевшим выехать в отделение ПАО «Сбербанк России» и получить следующую расширенную выписку о движении денежных средств по счету:*

1. У потерпевшего истребовать детализацию телефонных соединений с целью установления способа и направления перевода денежных средств.

2. Установить принадлежность абонентских номеров, используемых злоумышленниками в противоправных целях (запросить информацию в соответствующем оперативном подразделении органов внутренних дел или у оператора связи).

3. В случае создания учетной записи мобильного кошелька с использованием номера потерпевшего, в целях получения детализации транзакций осуществить вход в личный кабинет, SMS-сообщение с паролем поступит на телефон потерпевшего.

4. Согласно собранным документам, при наличии основания, указывающего на признаки соответствующей статьи УК РФ, принять решение о возбуждении уголовного дела.

5. В тех случаях, когда денежные средства поступают на счет абонентского номера, преступники производят их обналичивание через различные кредитные организации (платежные системы). В связи с этим необходимо направить запросы в финансовые организации для получения информации о владельцах счетов, на которые были переведены денежные средства.

6. Направить запрос в платежную систему для получения информации об IP-адресе администрирования и движении денежных средств. Запрос должен быть утвержден руководителем следственного органа и заверен гербовой печатью.

7. Изъять телефон у потерпевшего. Изъятие производится без SIM-карты потерпевшего, но с находящейся flash-картой или другим накопителем в телефоне. Изъятый телефон направить в экспертно-криминалистическое подразделение для производства дальнейшего исследования и получения необходимых ответов на интересующие органы дознания вопросы.

8. *С учетом возникшей ситуации необходимо перед экспертом поставить следующие вопросы:*

- имеются ли в памяти мобильного устройства и на flash-памяти программные продукты, детектируемые антивирусным программным обеспечением как вредоносные;

- если да, произвести копирование обнаруженных программных продуктов на неизменяемый оптический носитель информации.

Обязательно вносить после представленных вопросов следующие рекомендации: «Разрешаю внесение изменений в первоначальное состояние вещественного доказательства в объеме, необходимом для проведения исследования».

9. При получении информации о принадлежности абонентских номеров, а также о владельцах счетов (электронных платежных систем, банковских) необходимо подготовить ходатайство перед судом на получение технической информации:

- о соединениях интересующих абонентских номеров;
- о месте положения терминала сотовой связи в зоне действия конкретной базовой станции с привязкой к местности с целью установления фактического местонахождения злоумышленника в момент совершения противоправных действий;
- о движениях денежных средств по счетам с указанием суммы, реквизитов получателей и мест администрирования во время выполнения операций.

10. Получив судебные решения, истребовать необходимую информацию. В случае отсутствия филиала организации, владеющей информацией, запрос и судебное решение необходимо направить в структурное подразделение полиции по месту нахождения головного офиса.

11. Сотрудники, ответственные за формирование информационно-поисковой системы, осуществляют ввод информации в банк данных и ее корректировку при получении новых сведений.

По установлению конечного места завладения денежными средствами провести необходимые оперативно-розыскные мероприятия, направленные на отождествление личности злоумышленника.

Более сложные схемы хищения денежных средств

Далее представлены более сложные схемы совершения преступлений в системе ДБО.



Рис. 8. Разработка сложных схем хищения денежных средств «хакерами»



Рис. 9. Тактика хищения денежных средств



Рис. 9. Тактика хищения денежных средств (продолжение)

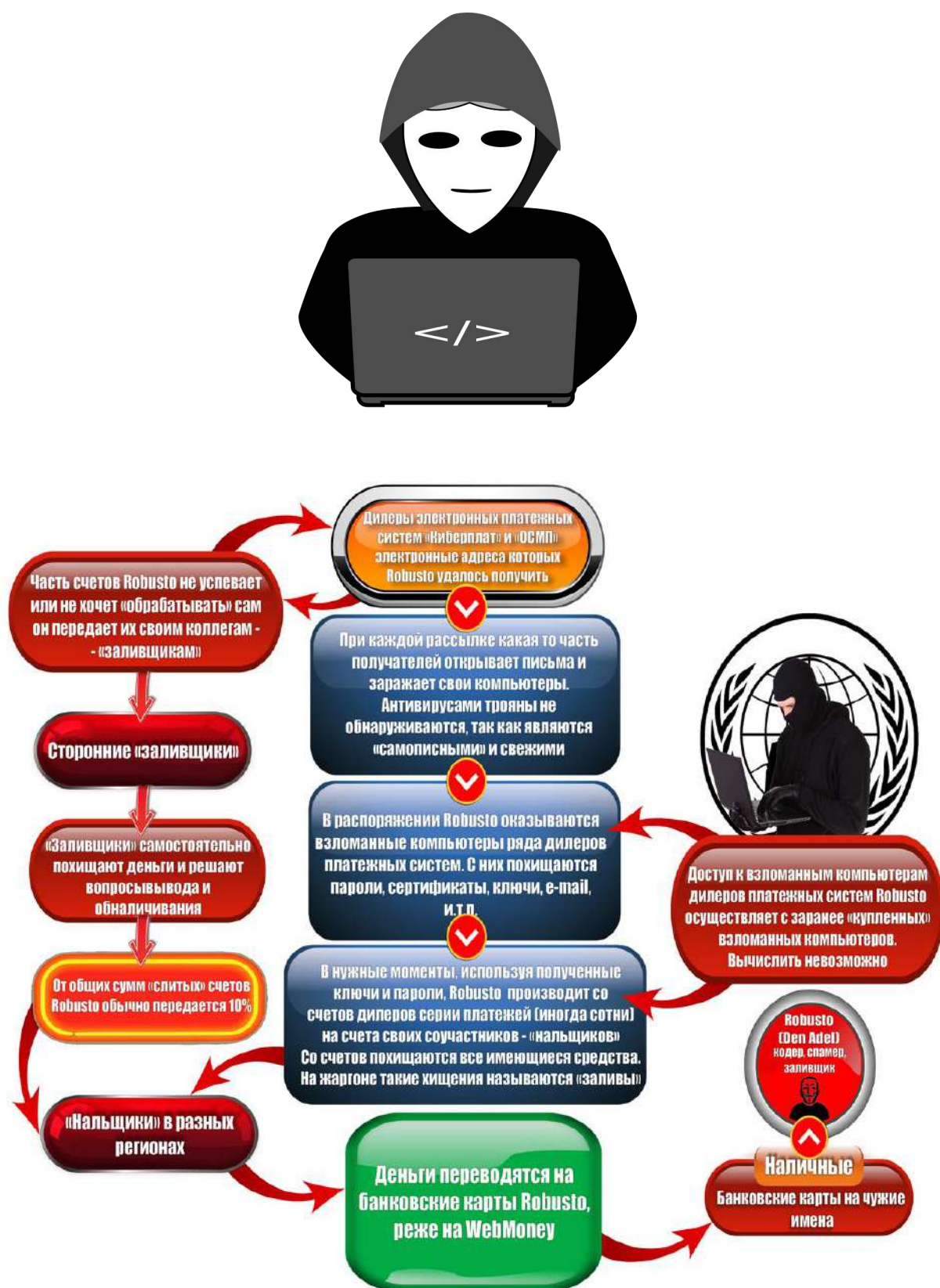


Рис. 9. Тактика хищения денежных средств (продолжение)

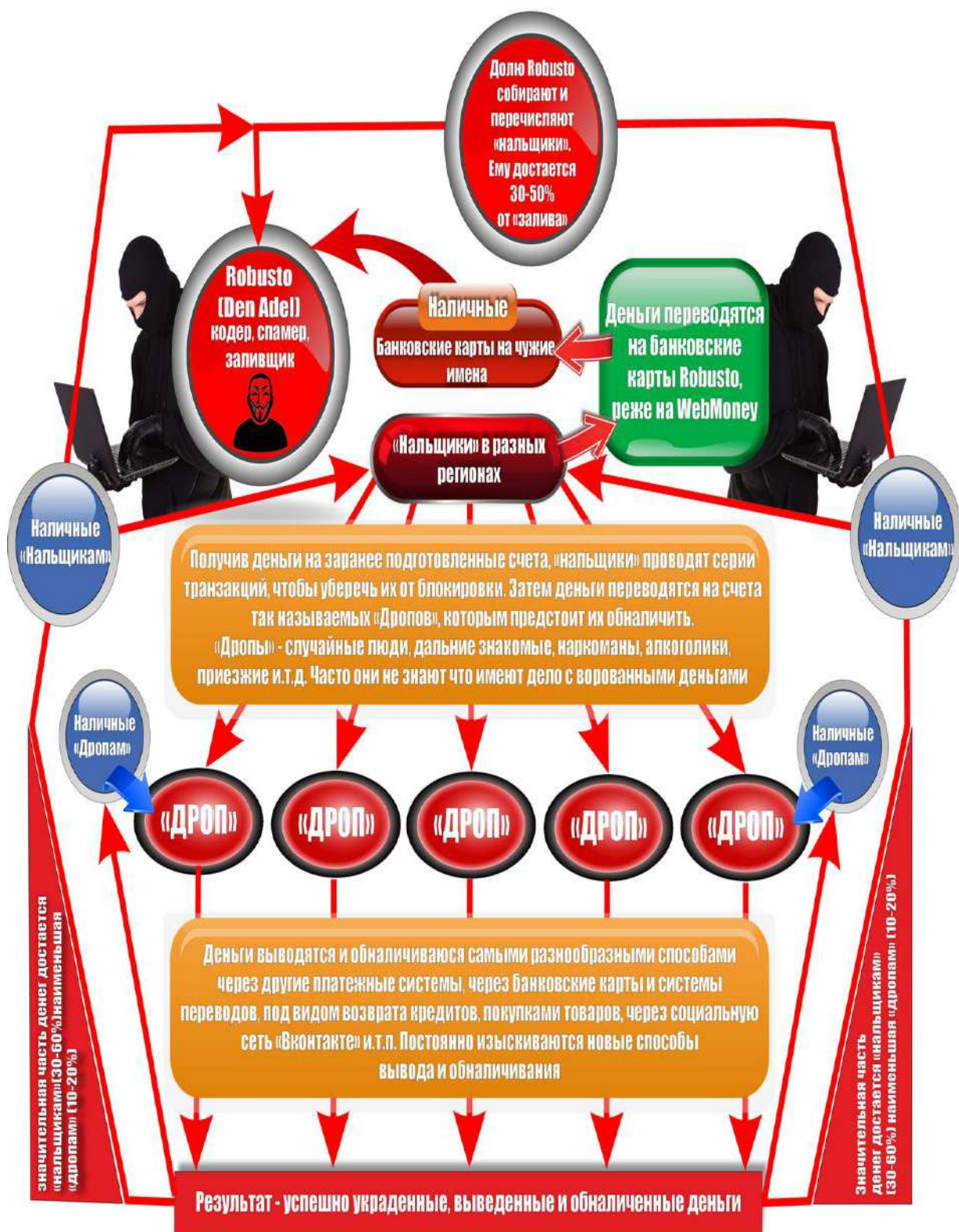


Рис. 9. Тактика хищения денежных средств (продолжение)

В одном из блоков схемы мы видим, что злоумышленники используют управляемые сети из зараженных компьютеров – так называемые «ботнеты» (сеть компьютеров, зараженных вредоносной программой, позволяющей киберпреступникам удаленно управлять зараженными машинами: каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком без ведома пользователя). На диаграмме 2 показано распределение зараженных компьютеров по категориям их деятельности в международной сети Интернет.

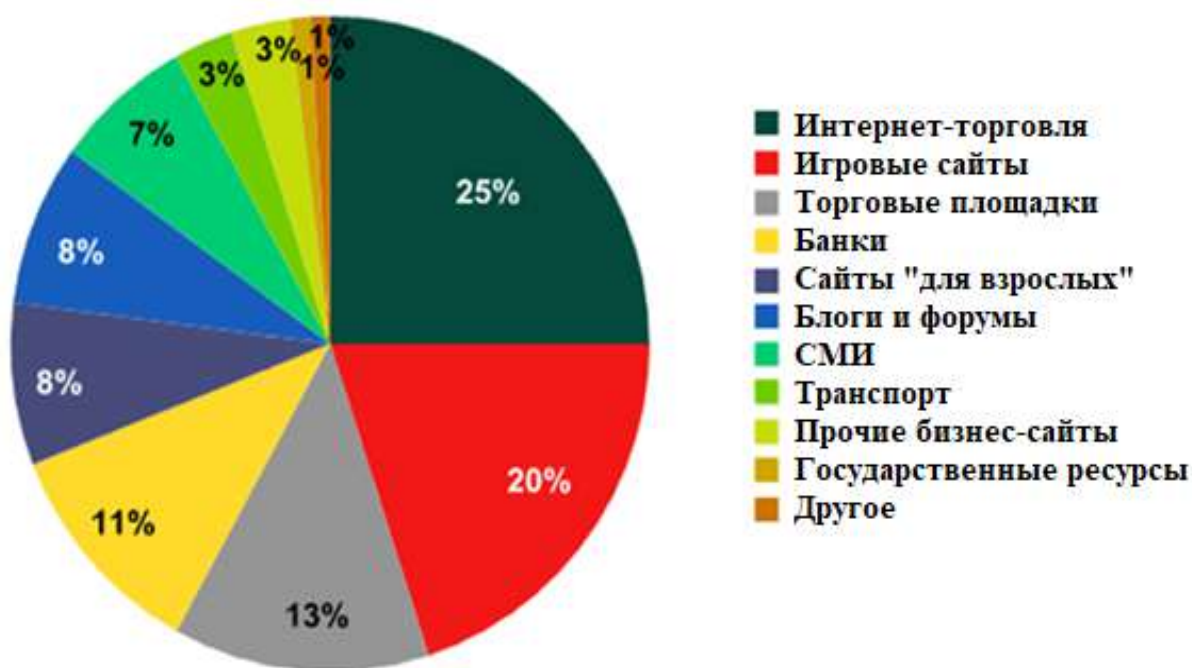


Диаграмма 2. Распределение атакованных ресурсов по категориям интернет-деятельности при хищении денежных средств

Таким образом, понятно, что наибольшему риску заражения для участия в управляемой злоумышленником сети подвержены сайты интернет-торговли и игровые сайты.

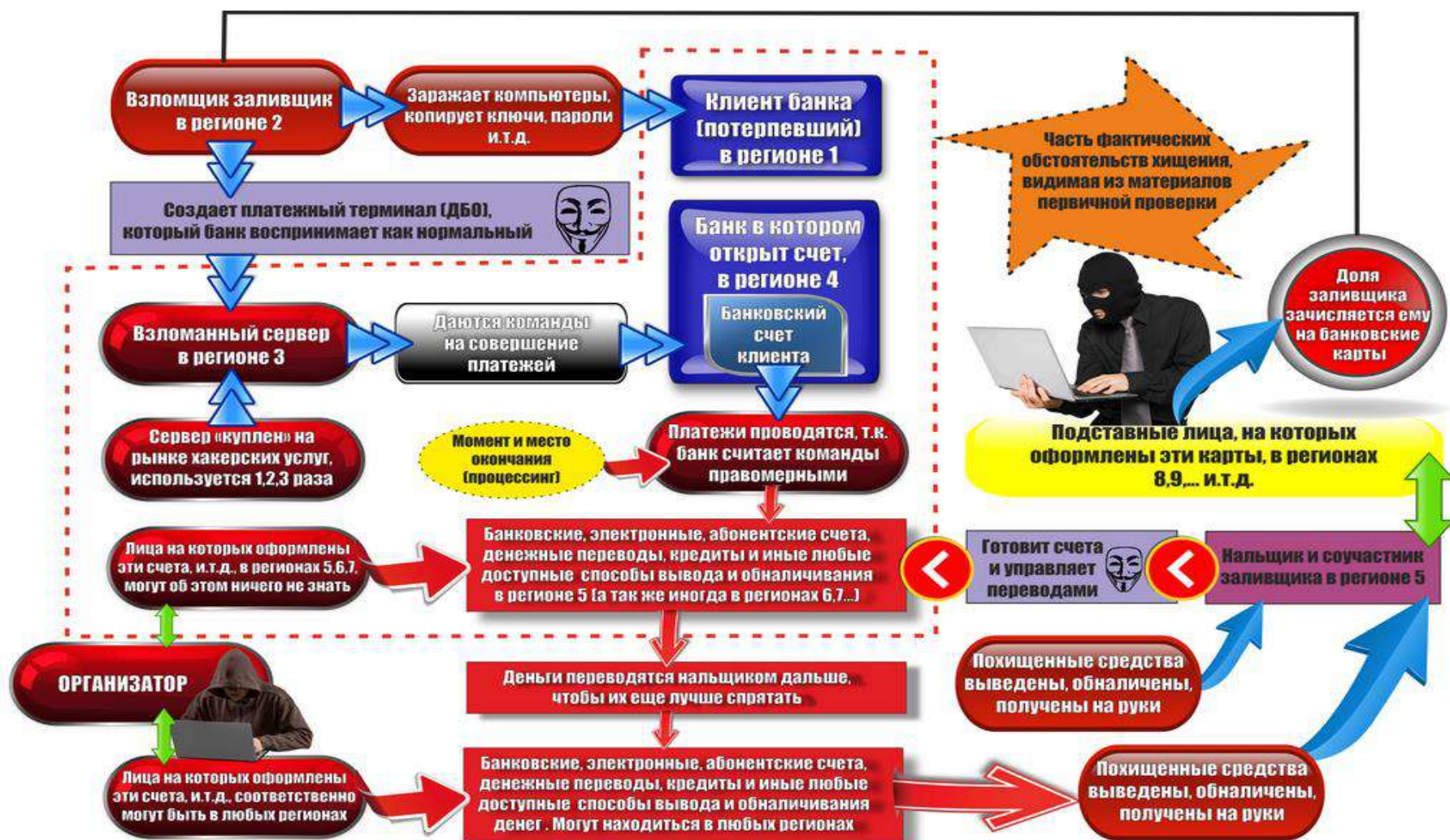


Рис. 10. Территориальная схема типового хищения

4.3. Особенности раскрытия преступлений, связанных с хищением денежных средств в системе дистанционного банковского обслуживания

Тактика раскрытия хищений денежных средств в системе ДБО

В случае поступления информации о совершенном хищении денежных средств со счета клиента банка в органы внутренних дел уполномоченным сотрудникам необходимо установить способ совершения хищения, а именно: выехать на место дислокации организации (компании или лица) для осуществления **осмотра** электронного устройства, на котором установлено ДБО.

В ходе проведения осмотра электронного устройства необходимо:

1. Выяснить, каким образом осуществляется подключение данного электронного устройства к сети Интернет.

2. Определить, какой вид ДБО установлен (у каждого банка свой вид ДБО).

3. Зафиксировать факт наличия подключенных и находящихся на месте «ключей» электронной цифровой подписи (ЭЦП). «Ключи» ЭЦП необходимы для проведения финансовых операций с использованием ДБО. Их количество может варьироваться от двух и более.

В ходе проведения первоначальных проверочных мероприятий установить или опровергнуть причастность к хищению денежных средств сотрудников данной организации (компании).

После чего необходимо опросить директора, главного бухгалтера, а также, при наличии в штате, администратора сети организации (компании). В ходе проведения опроса выше указанных лиц необходимо акцентировать внимание на получении следующей информации:

- кто имел и имеет доступ к электронному устройству, на котором установлено ДБО;

- не было ли замечено ими в период похищения денежных средств подозрительной активности на данном электронном устройстве (самостоятельное включение и выключение компьютера, непонятная активность курсора мыши на мониторе компьютера, зависание компьютера либо еще какие-либо события, ранее не происходившие);

- о точном времени составления и отправления платежного поручения, в результате чего были похищены денежные средства;

- в период хищения денежных средств подробно установить, чем занимались опрашиваемые лица, а также все те, кто имел или имеет доступ в обследуемое помещение, где находится компьютер;

- установить, каким способом компьютер подключается в сеть, а именно, возможно ли с него получение доступа в локальную сеть, либо он напрямую подключен в сеть Интернет;

- установить, ведется ли логирование доступа в сеть Интернет рабочих компьютеров организации, что обязательно необходимо для установления возможного неправомерного доступа в сеть организации из вне.

4. После вышеперечисленных действий в обязательном порядке данное электронное устройство, подвергшееся атаке, необходимо изъять для последующего проведения компьютерно-технической экспертизы.

5. По возможности до приезда следственно-оперативной группы связаться с пострадавшей организацией (компанией) и сообщить о необходимости отключения данного электронного устройства от локальной сети и сети Интернет, а также полного отключения электропитания.

6. Одновременно с целью получения информации о движении похищенных денежных средств связаться с банком, клиентом которого является пострадавшая организация (компания), заявившая, что с ее счета были похищены денежные средства.

7. Получить лог-файлы (информация об IP-адресе, дате и времени) доступа к системе «Клиент-Банк».

8. После завершения всех необходимых проверочных мероприятий, получения оперативно значимой и другой информации следует осуществить ее тщательный анализ.

9. Запросить у провайдера, оказывающего пострадавшей организации (компании) услуги доступа в сеть Интернет, детализированную статистику доступа в сеть Интернет (при необходимости получить судебное разрешение на получение этой информации); период получения запрашиваемой информации должен составлять около 7 дней.

10. Провести анализ полученной детализированной статистики. В ходе просмотра информации необходимо установить, какие IP-адреса обращались к IP-адресу организации (компании) в момент хищения, а также проверить информацию с целью получения сведений о совпадении IP-адресов за проверяемый период. При установлении «подозрительного» IP-адреса проанализировать объем переданной и полученной им информации, а также используемый порт, при его доступе к IP-адресу организации.

11. Необходимо получить информацию о принадлежности «подозрительного» IP-адреса. Если IP-адрес российский, направить запрос в организацию, которой он принадлежит, либо в НЦБ Интерпола.

12. Отработать информацию о движении денежных средств: куда и на какой счет были переведены похищенные денежные средства; был ли установлен факт их обналичивания; в случае подтверждения

интересующего события осуществить его документирование и сохранить видеозапись с банкоматов и камер видеонаблюдения.

Предлагаем рассмотреть понятия основных способов идентификации лиц, подозреваемых в совершении преступлений, в сети Интернет.

Основные способы идентификации преступника в сети Интернет (сведения об «IP-адресе» и «MAC-адресе»)

Сотрудники оперативных подразделений, в чьи должностные обязанности входит раскрытие преступлений, связанных с хищением денежных средств в системе ДБО, **обязаны знать** часто встречающиеся ключевые понятия, имеющие отношение к данной сфере. Предлагаем их рассмотреть.

Анонимизация – совокупность действий, направленных на сокрытие личности пользователя путем маскировки или подмены характеристик пользователя и его устройств.

Деанонимизация – совокупность действий, совершаемых лицом или автоматизированной системой, направленных на раскрытие реальной личности пользователя и характеристик его устройств.

Виртуальная личность – совокупность данных, характеризующих пользователя и представляющих его в Интернете: логин, аватар, почтовый адрес, подпись на форуме.

Анонимизированная личность – замаскированная виртуальная сущность, используемая для создания анонимности.

Субъект деанонимизации – тот, кто осуществляет деанонимизацию.

Объект деанонимизации – тот, деанонимизацию кого осуществляют.

VPN «виртуальная частная сеть» — это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

TOR – это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания.

Виртуальная машина – программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жесткий диск, привод, BIOS, сетевые адаптеры и т.д.).

Виртуальный сервер – услуга предоставления в аренду так называемого виртуального выделенного сервера. В плане управления операционной системой по большей части она соответствует физическому выделенному серверу.

Веб-сервер – сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-поток или другими данными.

IP-адрес (айпи-адрес, сокращение от англ. Internet Protocol Address) – сетевой адрес узла в компьютерной сети, построенной по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети.

MAC-адрес компьютера (электронного устройства) (от англ. Media Access Control – управление доступом к среде) – уникальный идентификатор, присваиваемый каждой единице активного оборудования (устройства) или некоторым их интерфейсам в компьютерных сетях Ethernet.

«IP-адрес» может быть статическим (постоянным) или динамическим (временным). В любом случае «IP-адрес» «привязан» к месту расположения устройства, выходящего в сеть, либо персональным данным лица, на чье имя заключался договор (при использовании мобильного Интернета). Сведения о том, кому был присвоен «IP-адрес», хранятся у поставщика услуг Интернета (например, компании «Ростелеком» и др.) и содержат данные о том, по какому адресу находится компьютер, с которого был осуществлен выход в сеть, информацию о лице, с которым был заключен договор о предоставлении услуг Интернета.

Таким образом, можно выделить две технологические основы, одна из них – инфраструктура пользователя (рис.11), то есть какой тип ЭВМ используется и как осуществляется доступ в сеть. Вторая технологическая основа – организация защиты, т.е. безопасность пользователя в процессе соединений (см. рис.12).

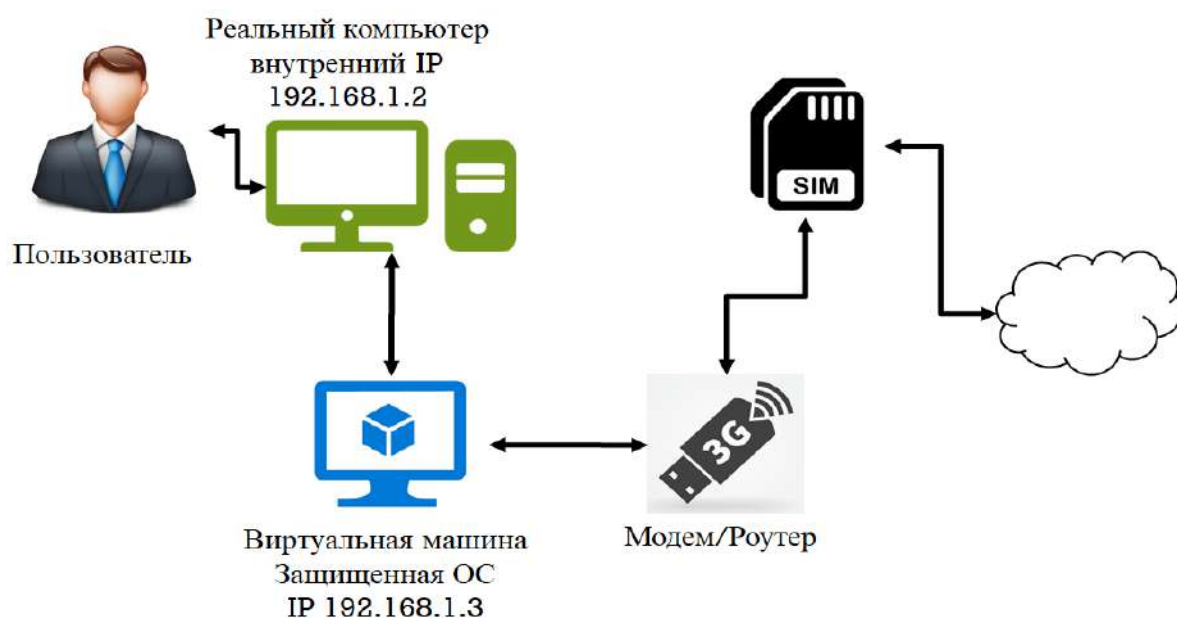


Рис. 11. Технические основы. Инфраструктура пользователя

Отсюда следует, что в случае установления «IP-адреса», с которого преступники выходили в сеть через проводной Интернет, компания-провайдер может предоставить сведения, как о месте расположения компьютера, так и о персональных данных лица, на чье имя заключался договор. Однако необходимо помнить, что подобные сведения хранятся непродолжительное время. **Период хранения зависит от технических возможностей провайдеров и может составлять от 1 месяца до нескольких лет. Поэтому промедление может привести к утрате важной информации¹⁴.**

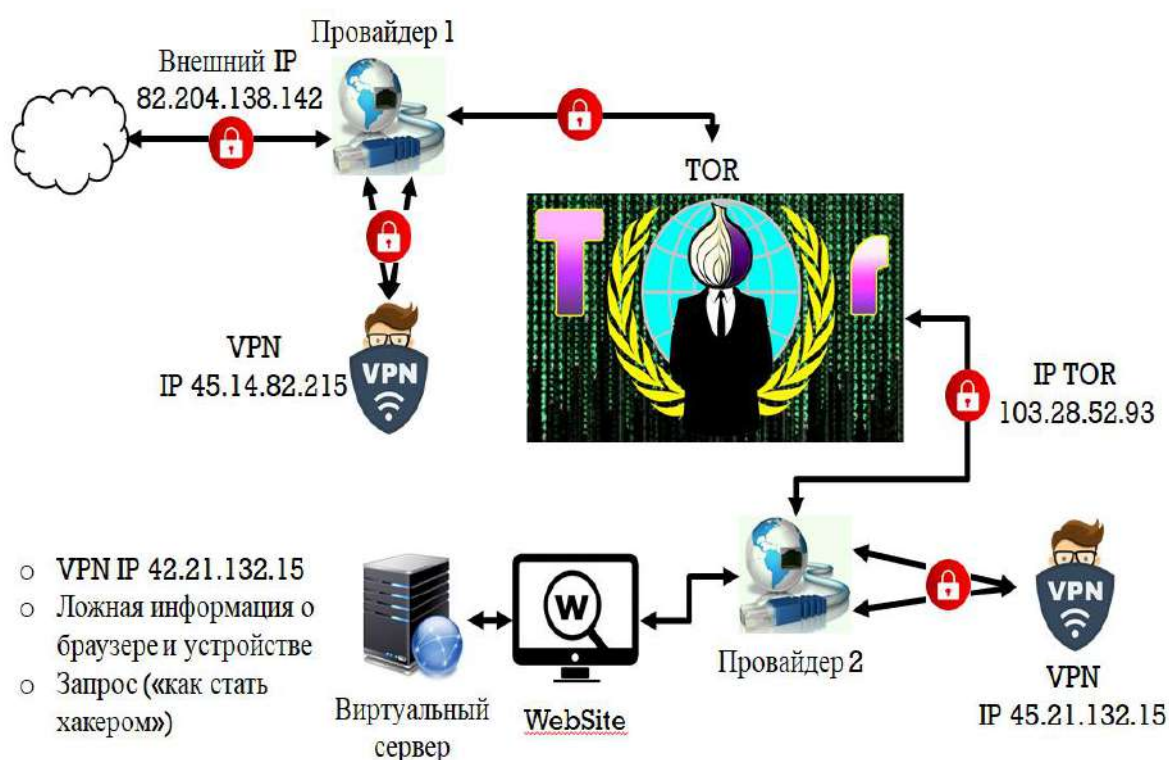


Рис. 12. Технические основы. Организация защиты

При использовании преступниками мобильного Интернета (через USB-модем или сотовый телефон) по известному сотрудникам органов внутренних дел «IP-адресу» компания-провайдер может предоставить

¹⁴ В соответствии с п. 12 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, утвержденными Постановлением Правительства Российской Федерации от 27 августа 2005 г. № 538, сведения об оказанных услугах связи должны храниться оператором в течение 3 лет. Однако, в ряде случаев операторы связи не соблюдают указанное требование, ссылаясь на отсутствие технических возможностей для хранения значительного объема информации.

сведения лишь о персональных данных лица, на чье имя заключался договор о предоставлении услуг связи при оформлении (приобретении) SIM-карты (см. рис. 13).

Определенные затруднения может вызвать ситуация, когда выход в сеть преступниками был осуществлен из так называемой «зоны свободного Wi-Fi»-участка. В нем Интернет предоставляется всем желающим бесплатно: территории крупных торговых центров, некоторые кафе, вагоны метрополитена и др., где каждый может воспользоваться услугами Интернета с любого портативного устройства (ноутбук, телефон). В этом случае по «IP-адресу» будут представлены лишь сведения о том, что доступ был осуществлен из зоны «Wi-Fi» по определенному адресу населенного пункта.

В качестве способа выявления лиц, осуществляющих выход в Интернет в преступных целях из «Wi-Fi»-зон, необходимо:

1. Анализировать видеозаписи с прилегающей территории (если таковая ведется) и осуществлять последующую проверку выявленных лиц, используемого автотранспорта.

2. Сопоставлять «MAC-адрес» изъятых у подозреваемых электронных коммуникационных устройств с теми, которые были зафиксированы при совершении рассматриваемых видов преступлений.

Несмотря на то, что «MAC-адрес» может быть незаконно изменен пользователем в попытке уйти от контроля, существует вероятность выхода компьютера преступника в сеть в нескольких точках доступа с одним и тем же «MAC-адресом». Например, используется ноутбук, который периодически **приносят в одну или различные зоны «Wi-Fi», либо с него выходят в сеть, используя проводной Интернет в различных стационарных точках доступа (квартиры, офисы).**

В целях получения информации, представляющей оперативный интерес, необходимо запросить компании, ранее предоставляющие доступ в сеть Интернет по установлению «IP-адресов» (место, территория), у которых был зарегистрирован выход компьютера в сеть с «MAC-адресом» (серийный номер устройства).

Также еще одним из способов разоблачения преступника является установление все учетных данных в сети Интернет, но часто это осложняется нахождением виртуальной личности, а также личности, которая может быть анонимизированной (см. рис. 13).



Рис. 13. Пример виртуальной личности

Особенности предоставления услуг «хостинга» в сети Интернет при создании сайтов преступниками

В случае создания вымышленных «сайтов», например, «зеркальных» сайтов, рассмотренных выше, преступники могут пользоваться ячейками. Данные ячейки выделяются администрацией крупных сайтов для размещения на них своих небольших по объему страниц – **мини-сайтов** (услуги «хостинга»). Услуги «хостинга» в большинстве случаев оплачиваются, что позволяет установить, с каких счетов преступниками перечислялись денежные средства. Кроме того, создателю страницы сайта предоставляется право выхода и администрирования, что позволяет установить «IP-адреса», с которых преступники управляли сайтом. Помимо IP-данных, зафиксированных при создании и последующем управлении сайтом, **злоумышленники могут регистрироваться в администрации хостинга**, указывая почтовый ящик (E-mail). Данный E-mail они могут использовать несколько раз при создании сайтов, а также для ведения собственной переписки. Вся информация технического и организационного характера от организации (компании), предоставляющей услуги хостинга, будет направляться на данный почтовый ящик E-mail. Полученную информацию в дальнейшем следует учитывать при доказывании вины преступников. Злоумышленники вынуждены периодически проверять почту, а также отвечать организатору хостинга по вопросам функционирования страницы своего сайта.

В связи с этим необходимо направлять запросы в компании, предоставляющие ресурсы, на которых преступники размещали данные сайты. Целью направляемых запросов является: установление «IP-адресов» и «MAC-адресов» регистрации сайта, управление сайтом, сведений об оплате услуг, адреса использовавшейся электронной почты. Вся полученная информация подвергается глубокому анализу для последующего общего сбора оперативной и доказательственной информации, а также посредством проведения оперативно-розыскного мероприятия «снятие информации с технических каналов связи».

Особенности предоставления операторами сотовой связи дополнительных услуг абонентам

Зачастую, при совершении хищений денежных средств, преступниками в качестве своеобразной платежной системы используются счета абонентских номеров сотовой связи. Их выбор объясняется относительной простотой перевода денежных средств, а также легкой возможностью управления счетом телефонного номера через «личный кабинет» в сети Интернет для дальнейшего перечисления похищенных денежных средств. В случае перечисления преступниками похищенных денежных средств на телефонные номера сотовой связи необходимо через соответствующие структурные подразделения органов внутренних дел направить запрос в компании, предоставляющие услуги связи. Целью запроса является: установление телефонных номеров или иных счетов, на которые были перечислены денежные средства со счета данного телефонного номера, кем и где данные средства были обналичены.

Таким образом, своевременность и качество выявления и раскрытия хищений денежных средств, совершенных с использованием вредоносных программ, напрямую **зависит** от учета **специфики способов** совершения преступлений, предоставления операторами сотовой связи дополнительных услуг абонентам и средств идентификации преступника в сети Интернет. По выполнению всех первоначальных мероприятий и получении необходимой информации оперативный сотрудник избирает тактически грамотную линию своего поведения и акцентирует работу на дальнейшую организацию и планирование хода раскрытия преступлений.

Особенности опроса потерпевшего

Заявление (сообщение), поступившее в орган внутренних дел о факте хищения денежных средств с банковской карты (расчетного счета), подлежит регистрации в установленном порядке¹⁵. После этого необходимо составить план проведения первоначальных оперативно-розыскных мероприятий и следственных действий.

¹⁵ Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях: приказ МВД России от 29.08.2014 № 736.

В ходе опроса заявителя (потерпевшего) **в объяснении необходимо отразить:**

- каким образом, где и при каких обстоятельствах стало известно о хищении денежных средств с банковской карты (расчетного счета);
- время обнаружения пропажи денежных средств и в какой сумме;
- номер банковской карты и (или) банковского счета, с которого были похищены денежные средства, наименование банка;
- адресат, куда переведены денежные средства (абонентский номер сотового телефона или банковский счет, используемая платежная система и т.д.);
- название и модель используемого сотового телефона, где и когда приобретался, имеются ли соответствующие документы (кассовый, товарный чек);
- каким образом, где и при каких обстоятельствах была подключена услуга «Мобильный банк», «Сбербанк Онлайн»: дата подключения, «привязка» к абонентскому номеру;
- факт поступления SMS-сообщений на сотовый телефон от имени каких-либо банковских учреждений, если да, то когда и при каких обстоятельствах;
- факты поступления SMS-сообщений со ссылками на интернет-страницу, если да, то когда и какого содержания;
- используемые на сотовом телефоне интернет-ресурсы: «Одноклассники», «Вконтакте», «Play Маркет» и т.д.

При принятии заявления и отборе объяснения у потерпевшего необходимо установить все обстоятельства и определить, каким способом произошло хищение денежных средств. *Кроме того, необходимо выяснить:*

1. Обращался ли потерпевший по факту данного хищения денежных средств в банк?
2. Если да, то каким образом он обращался и в какой форме представители банка ему ответили?
3. Были ли предприняты какие-либо меры со стороны представителей банка после обращения потерпевшего? Если да, то как быстро произошло реагирование на информацию заявителя?

Часто при получении SMS-сообщения о снятии денежных средств со счета потерпевшие обращаются по телефону в банк, где операторы обратившемуся клиенту сообщают, куда были перечислены денежные средства, с какого номера телефона было отправлено SMS-сообщение, и иногда сообщают абонентский номер, на счет которого перечислены денежные средства.

Для принятия соответствующих мер по возврату похищенных денежных средств, а также ускорения получения информации об обстоятельствах преступления потерпевшему необходимо в кратчайшие сроки

связаться с представителями банка. Далее потерпевшему оперативные сотрудники рекомендуют подготовить и направить сотрудникам банка заявление об отмене платежа и получить справку по факту инцидента¹⁶. В случае, если у потерпевшего имеется детализация звонков и SMS-сообщений от оператора сотовой связи, а также выписка из лицевого счета, необходимо данные документы (или копии) приобщить к имеющимся проверочным материалам. **Обязательным условием** при первичном опросе потерпевшего является **получение и приобщение вышеуказанных документов** к материалам проверки. По окончании опроса потерпевшему разъясняется право имеющейся возможности обращения в суд с исковым заявлением о взыскании похищенных денежных средств с обслуживающего его банка¹⁷.

Виды запросов подразделений МВД России в Сбербанк России

При получении от потерпевших информации о банковских счетах или банковских картах, а также другой информации, касающейся банковских услуг, сотрудники органов внутренних дел отправляют в банки, в частности в Сбербанк России, соответствующие запросы. Чаще всего оперативные сотрудники осуществляют тесное взаимодействие со Сбербанком России.

В процессе сотрудничества соответствующих подразделений МВД России может направить в Сбербанк России **три вида запросов** (см. рис. 14).

Первый вид запроса – это получение информации оперативными сотрудниками органов внутренних дел о банковской карте (банковском счете) потерпевшего или злоумышленника.

Если в дальнейшем от Сбербанка России поступает ответ, что данная карта (или счет) принадлежит банку, необходимо установить следующую информацию об отправителе средств:

- установочные данные;
- дату/время, сумму операции /выписка/;
- через какой сервис (Яндекс, ЮНИСТРИМ и прочие) была совершена операция.

Если от Сбербанка России поступает отрицательный ответ, то в этом случае запросы осуществляются в другие банки.

Второй вид запроса – это получение информации оперативными сотрудниками органов внутренних дел о сервисе Сбербанка России.

¹⁶ Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента. Утверждены Рабочей группой Ассоциации Российских банков (2012). Доступ из СПС «КонсультантПлюс».

¹⁷ ГК РФ. Ст. 845, 849, 854.

В том случае, когда от Сбербанка России поступает на указанный запрос положительный ответ, необходимо выяснить информацию о принадлежности сервиса:

- СБОЛ (Сбербанк Онлайн – IP-адрес);
- СБОЛ МП (мобильное приложение «Сбербанк Онлайн» – IP-адрес);
- МБК (Мобильный банк);
- УС (установочные данные – номер, место установки, фото-, видео – при наличии).

В случае отсутствия данных Сбербанк России может предоставить информацию об организации, владельце сервиса.

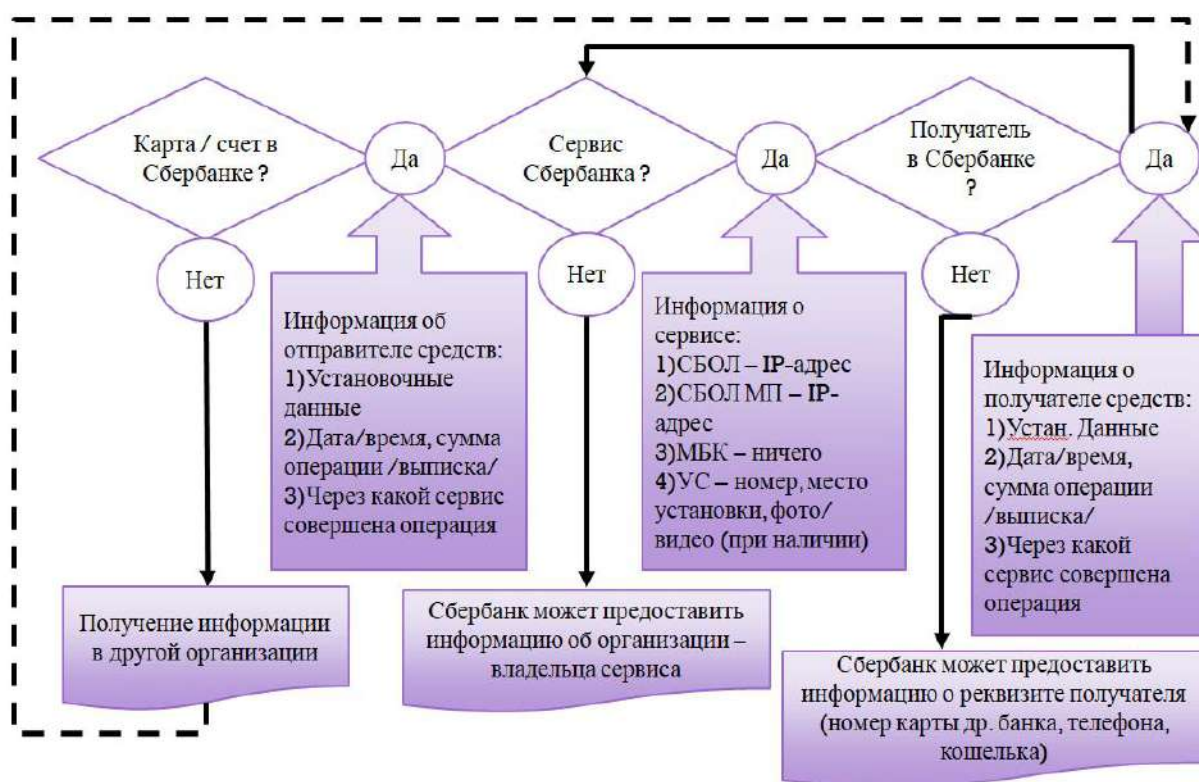


Рис. 14. Виды запросов подразделений МВД России в Сбербанк России

Третий вид запроса проводится, когда у оперативных сотрудников органов внутренних дел имеется информация о получателе Сбербанка России.

При поступлении положительного ответа необходимо установить следующую информацию о получателе средств:

- установочные данные;
- дату/время, сумму операции /выписка/;
- через какой сервис совершена операция.

Если отсутствуют интересующие оперативных сотрудников конкретные данные, то в этом случае Сбербанк России может предоставить информацию о реквизите получателя (номер карты другого банка, номер телефона, кошелек).

Изъятие сотового телефона и flash-карты.

После опроса потерпевшего необходимо изъять сотовый телефон и flash-карту¹⁸.

Изъятие мобильного телефона чаще всего производится без SIM-карты потерпевшего, поскольку она в ряде случаев не несет информации, требующей исследования. Находящуюся в телефоне flash-карту или другой накопитель информации необходимо изъять, так как они могут содержать внедренные преступниками вирусы или следы их действия.

Изъятый телефон направляется в экспертно-криминалистическое подразделение для проведения компьютерного исследования и установления наличия в памяти устройства вредоносных программ, определения задач, механизма и особенностей действия.

В случае получения от эксперта неполного ответа на все указанные вопросы (например, если было установлено лишь наличие следов вредоносной программы, которая самостоятельно удалилась из памяти устройства; программа обнаружена, но не выявлен механизм ее действия), возможно проведение дополнительных исследований в сторонних организациях или иных экспертно-криминалистических подразделениях. Независимо от фактической полноты проведенного исследования, его результаты имеют значение для квалификации деяния, и полученные результаты подлежат обязательному приобщению к материалам предварительной проверки, содержащим признаки состава преступления¹⁹. Данные материалы в ходе предварительного расследования могут быть признаны вещественными доказательствами, что положительно скажется на раскрытии преступления.

¹⁸ Изъятие телефона у потерпевшего для последующего исследования, исходя из содержания действий сотрудников полиции, должно оформляться протоколом изъятия (ч. 1 ст. 15 Федерального закона «Об ОРД»).

¹⁹ По результатам проведения предварительной проверки в порядке ст.144 УПК РФ и установления признаков состава преступления, предусмотренного ч.1 или ч.2 ст.158 УК РФ, материалы могут направляться по подследственности для возбуждения уголовного дела. После получения результатов компьютерного исследования и соответствующих экспертиз деяние может быть дополнительно квалифицировано по ст.272, 273 УК РФ.

Оперативно-розыскные мероприятия, проводимые при установлении факта перечисления денежных средств на абонентский номер сотового оператора

При установлении факта перечисления денежных средств на абонентский номер сотового оператора проводятся следующие оперативно-розыскные мероприятия²⁰:

– ОРМ «Наведение справок» по абонентским номерам, на которые осуществлен перевод денежных средств, путем обращения к базам данных и использования справочных программ в сети Интернет в целях установления региона, к которому они относятся, а также персональных данных владельца. Данные мероприятия необходимы для определения региона, в котором зарегистрирован абонентский номер. После проведенного анализа собранных материалов полученная информация направляется в территориальный орган внутренних дел того региона, к которому относится абонентский номер, и производится запрос в сотовую компанию с целью получения имеющейся информации.

При этом необходимо учитывать, что полученные в ходе **предварительной проверки сообщения о преступлении**, сведения о фамилии, имени, отчестве абонента-гражданина, наименовании фирмы абонента – юридического лица, фамилии, имени, отчестве руководителя и работников этого юридического лица, а также об адресе абонента, абонентских номерах, не ограничивают право лица на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; установление данной информации осуществляется без судебного решения путем проведения гласного оперативно-розыскного мероприятия «Наведение справок».

– ОРМ «Наведение справок» о владельце абонентского номера о учетам «ИБД-Р», «ИБД-Ф», «ПТК Розыск-Магистраль», в социальных сетях Интернета, для подтверждения факта существования такого лица, его регистрации по месту жительства на территории региона, получения фотографии указанного лица.

– ОРМ «Снятие информации с технических каналов связи». В данном случае необходимо подготовить и направить в суд ходатайство на получение судебного решения на проведение мероприятия «Снятие информации с технических каналов связи» об абонентских номерах, на которые были переведены денежные средства.

В случае получения информации о нахождении абонента сотовой сети в другом регионе, необходимо подготовить и направить в установленном порядке весь собранный материал по территориальности.

В подготовленном материале, представляющем оперативный интерес и требующем дополнительной проверки, рекомендовать уточнить

²⁰ Далее – «ОРМ».

анкетные данные установленных лиц по учетам, выявить их местонахождение с последующим проведением опроса и обязательным выяснением следующих обстоятельств:

- когда, где и при каких обстоятельствах была приобретена SIM-карта;
- какими сведениями располагает опрашиваемый о лице, использующем SIM-карту;
- где находился опрашиваемый в момент совершения преступления.

В результате проведенных оперативно-розыскных мероприятий и полученной информации:

- о местонахождении абонентских номеров, на которые происходило зачисление денежных средств в момент совершения преступления, а также в последующий период;
- о базовых станциях, через которые происходило соединение, и их местоположении;
- об азимуте направления;
- о сведениях, содержащих входящие и исходящие соединения;
- об IMEI-коде мобильного устройства, регистрировавшегося с абонентским номером, IMSI (идентификационный номер SIM-карты);
- о входящих и исходящих SMS-сообщениях, –

должностное лицо в праве самостоятельно расширять круг устанавливаемых обстоятельств, имеющих отношение к преступной деятельности.

С целью установления всех обстоятельств совершенного преступления необходимо направить в различные кредитные организации (платежные системы ООО НКО «МОБИ.Деньги», АО «Национальная сервисная компания», NanduQ, АО КБ «Юнистрим» и другие) запросы о маршруте перечисления похищенных денежных средств, способе их обналичивания, а также о получателе платежа.

Перечень рассмотренных оперативно-розыскных мероприятий может быть расширен в зависимости от возникшей на конкретный промежуток времени ситуации.

Получение оперативно значимых сведений оперативным сотрудником по учетным записям «электронного кошелька»

Необходимо установить следующие сведения о движении средств по учетной записи «электронного кошелька»:

- откуда поступали деньги, в каком объеме и в какой период;
- с какого «электронного кошелька» и кем осуществлялась операция;
- какие при этом использовались терминалы;
- с помощью какой платежной системы или банка осуществлялась операция.

Движение средств по учетной записи «электронного кошелька» также позволяет установить:

- куда и когда переведены деньги;
- за какие услуги и товары переведены денежные средства;
- в какую платежную систему (банк) они были переведены.

Сведения об IP-адресе компьютера, с которого управляли «электронным кошельком», **позволяют установить адрес объекта** (через провайдера), выяснить, какими еще «кошельками» управляли с этого IP-адреса.

Информация об UDID²¹-коде телефона, создающемся для устройств компании Apple на основе Apple-ID²², дает возможность узнать, какие еще «электронные кошельки» управлялись с данного устройства.

Сведения о MAC-адресе, данных зоны Wi-Fi **позволяют установить** место (места), **откуда пользователь «выходил»** в Интернет для управления «электронным кошельком», а также *идентифицировать* электронное устройство в случае его изъятия.

В данной ситуации мы считаем необходимым уточнить понятие идентификации, так как этот вопрос вызывает затруднение и носит спорный характер.

С этой целью нами предпринята попытка сформулировать свое видение на данное понятие: **криминалистическая идентификация – криминалистический способ познания, в основе которого лежит процесс сравнительного исследования как минимум двух объектов, причинно связанных с расследуемым преступным событием, с целью использования полученных результатов в ходе расследования и успешного раскрытия преступлений.**

Данные о «привязке» банковских карт (их банковских счетов) к «электронному кошельку» дают возможность установить, счета каких пластиковых карт и каких банков «привязаны» к «электронному кошельку».

По этим данным можно установить, какие именно платежи проводились, когда и в каком объеме, по каким реквизитам.

Установление регистрационных данных владельца «электронного кошелька» позволяет использовать сведения, которые указал пользователь при регистрации электронного счета («кошелька»):

- персональные данные – фамилию, имя отчество;
- основные и дополнительные телефоны;
- адреса электронной почты и т.д.;
- IP-адреса, с которых осуществлялась регистрация.

²¹ UDID – уникальный идентификатор устройства, состоящий из 40 символов. Он есть у каждого мобильного устройства категории iPad, iPhone или iPodTouch.

²² Apple-ID – персональный идентификатор в системе AppleiTunes и AppStore/ Он имеет вид почтового ящика E-mail, который пользователь самостоятельно регистрирует в специальной программе iTunes, где указывает действующий E-mail и некоторые персональные данные.

Получение оперативно значимых сведений оперативным сотрудником по платежам в терминалах

При получении информации, содержащей сведения, указывающие, где, когда, кем и на какую сумму пополнялся счет, «привязанный» к мобильному телефону абонента, можно установить историю (периодичность) пополнения данного счета, а именно: в каком терминале, когда (с точностью до секунд) и на какую сумму производилось пополнение счета, «привязанного» к конкретному мобильному телефону. Это позволит определить место, в котором находился объект в конкретный момент.

Сведения об иных платежах объекта дают возможность выявить его «вторые» телефоны, либо телефоны его связей, что создает необходимость проведения такого оперативно-розыскного мероприятия, как «Прослушивание телефонных переговоров».

Данные о том, где объект совершает платежи (по регулярному использованию одного терминала или рядом расположенных терминалов) **позволяют сделать предположение** о местонахождении объекта: по платежам в позднее и раннее время – о примерном месте жительства; по платежам в дневное время – о примерном месте работы (учебы) или ориентировочной территории нахождения объекта в то или иное время.

В целях предупреждения хищений терминалы устанавливают в местах, оборудованных камерами видеонаблюдения. По записям с камер видеонаблюдения (супермаркеты, магазины, стоянки, торговые центры) можно установить время и место платежа в терминале, определить лицо, осуществляющее платеж, автотранспортное средство и лиц, находящихся поблизости.

Работа по запросам продолжается до тех пор, пока не будет получен ответ о фактическом снятии денежных средств подозреваемыми лицами через банкомат или в филиале банка.

При необходимости продления срока проверки по имеющимся материалам, содержащим сообщение о преступлении, возникает необходимость проведения соответствующих оперативно-розыскных мероприятий и получения их результатов; в соответствии с ч. 3 ст. 144 УПК РФ выносится мотивированное постановление с ходатайством перед руководителем органа дознания о продлении срока проверки до 10 суток. В дальнейшем при развитии оперативно-розыскной ситуации и постоянно поступающей информации, представляющей оперативный интерес, выносится мотивированное постановление с ходатайством перед прокурором о продлении срока проверки до 30 суток.

Постановление о продлении срока проверки должно быть мотивированным. В нем необходимо указать **вид** проводимого оперативно-розыскного мероприятия, а также **цель** и **основания** проведения ОРМ.

В случае, если потерпевший по каким-либо причинам не может предоставить детализацию о движении похищенных денежных средств, необходимо подготовить и направить в районный суд ходатайство о получении судебного решения на предоставление исчерпывающей информации по движению денежных средств со счета.

Действия оперативного сотрудника в случае установления факта перечисления денежных средств на банковские счета

Установив номер банковского счета (банковской карты), необходимо в кредитной организации запросить следующую информацию:

- о персональных данных лица (организации), на чье имя выпущена банковская карта (открыт счет); при возможности запросить копии документов, предоставленных лицом при оформлении договора;
- о транзакциях, осуществленных по карте (счету) за анализируемый период, с указанием мест снятия денежных средств;
- о месте открытия и обслуживания карты, а также данные расчетного счета (с указанием номера офиса банка и адреса его местонахождения);
- о подключении услуги оповещения или услуги «Мобильный банк» к банковской карте и расчетному счету, с указанием всех абонентских номеров и адресов электронной почты.

При получении ответа из банка и установлении мест снятия денежных средств, необходимо незамедлительно направить запрос на получение видео- и фотоизображений из банкоматов и помещений, где установлены банкоматы, так как сроки их хранения ограничены.

В случае неполучения своевременного ответа от организации на направленный запрос о предоставлении информации существует возможность привлечения к административной ответственности виновных лиц по ст. 19.7 КоАП РФ «Непредставление сведений (информации)».

Таким образом, основными оперативно-розыскными мероприятиями, проводимыми для выявления и раскрытия хищений денежных средств со счетов клиентов банков, совершенных при помощи вредоносных программ, являются опрос потерпевшего, исследование изъятого сотового телефона и flash-карты, наведение справок и снятие информации с технических каналов связи.

4.4. Особенности производства отдельных следственных действий на начальном этапе расследования преступлений, совершаемых в системе дистанционного банковского обслуживания

Некоторые следственные действия, проводимые в ходе расследования хищений денежных средств, совершаемых в системе дистанционного банковского обслуживания.

В ходе раскрытия преступлений, совершаемых в системе ДБО, необходимо проводить, наряду с оперативно-розыскными мероприятиями, следующие, наиболее часто осуществляемые, следственные действия, такие как:

1. Осмотр места происшествия.

Данное следственное действие является одним из самых значимых и распространенных. *В ходе его производства следует обращать внимание на источники информации, которыми могут быть:*

- компьютеры, ноутбуки, моноблоки;
- носители информации (накопители на flash-памяти), карты памяти и т.д.;
- смартфоны, мобильные устройства, планшеты и т.д.;
- всевозможные журналы регистрации событий от интернет-провайдера;
- журналы регистрации событий от кредитной организации, предоставляющей систему ДБО²³.

Рассматривая данные объекты, можно уточнить и получить разъяснения на следующие вопросы:

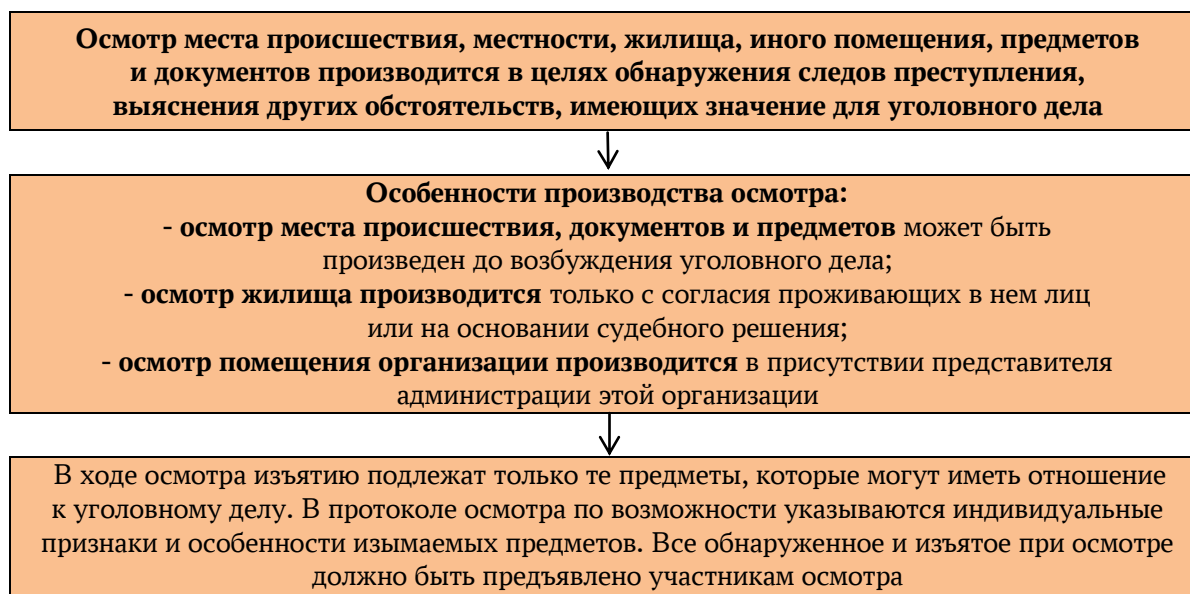
- с кем осуществлялась переписка в социальных сетях, на интернет-ресурсах, в программах для мгновенного обмена сообщениями;
- какие посещались интернет-сайты, в том числе в период совершения хищений;
- какие производились поисковые запросы;
- установлены ли на изъятых объектах вредоносные программы;
- можно ли получить сведения о подключаемых пользователях;
- можно ли получить информацию о сетевых соединениях и запущенных процессах;
- можно ли получить сведения об организации и фактическом лице, на имя которого был осуществлен платеж.

Предлагаем рассмотреть схему «Основания и порядок производства осмотра» согласно нормам ст. 176, 177 УПК РФ²⁴ (см. схема 1).

²³ Шмонин А.В., Баранов В.В. Организация выявления, раскрытия и расследование хищений денежных средств в системе дистанционного банковского обслуживания: учебно-практическое пособие / под науч. ред. доктора юридических наук, профессора А.В. Шмониной. М.: Академия управления МВД России, 2014.

²⁴ Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. М.: Проспект, 2021.

Основания и порядок производства осмотра (ст. 176, 177 УПК РФ)



2. Обыск и выемка.

Данное следственное действие, именуемое обыском, при расследовании рассматриваемого вида преступлений носит весьма специфичный характер и является чуть ли не основным средством доказывания, который заключается в обследовании помещений (жилища). Его целью является отыскание и изъятие объектов, причинно связанных с расследуемым преступлением. Таковыми могут быть предметы электронных носителей информации, компьютерная информация, различного рода документы, например, поддельные учредительные, регистрационные, банковские карты, похищенные денежные средства.

Все вышеперечисленные обнаруженные и в последующем изъятые объекты могут быть признаны в виде источников доказательств и использованы в процессе доказывания, а также приобщены к материалам уголовного дела, что может послужить в дальнейшем его раскрытию. В ряде случаев при производстве данного следственного действия, носящего принудительный характер, могут быть обнаружены и задержаны лица, скрывающиеся от правосудия.

Отличительной особенностью обыска от выемки является то, что при производстве (осуществлении) выемки категорически запрещается ведение поисковых действий.

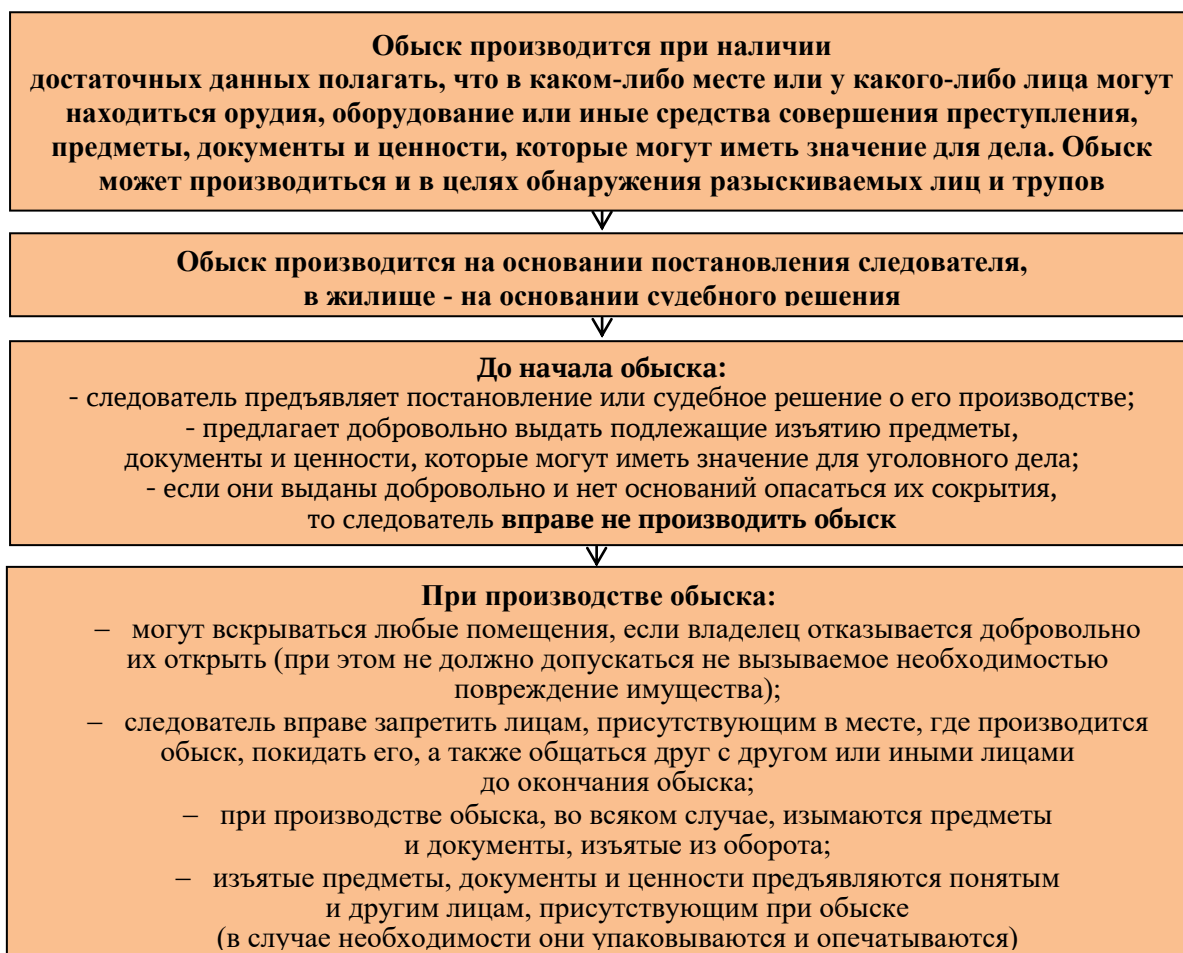
В ходе производства обыска и выемки все значимые объекты, которые по внутреннему убеждению сотрудников органов внутренних дел, входящих в оперативно-следственную группу, могут иметь доказательственное значение, подлежат изъятию при непосредственном участии понятых и в присутствии специалиста.

В случае поступления ходатайства от законного владельца обнаруженных и изымаемых объектов – электронных носителей информации – возможно удовлетворение его ходатайства и проведение копирования информации, но лишь в тех случаях, когда это действие не приведет к воспрепятствованию расследования преступления и не повлечет утрату или не изменит информацию. Затем сделанные копии передаются законному владельцу, а в протоколе обыска или выемки согласно ч. 1 ст. 182, ч. 3.1 ст. 183 УПК делается соответствующая запись.

Предлагаем рассмотреть схемы «Основания и порядок производства обыска» согласно нормам ст. 182 УПК РФ²⁵ (см. схему 2) и «Основания и порядок производства выемки» согласно нормам ст. 183 УПК РФ²⁶ (см. схему 3).

Схема 2

Основания и порядок производства обыска (ст. 182 УПК РФ)



²⁵ Шаталов А.С. Указ. раб. – С. 312.

²⁶ Там же – С. 315.

Основания и порядок производства выемки (ст. 183 УПК РФ)

При необходимости изъятия определенных предметов и документов, имеющих значение для уголовного дела, и если точно известно, где и у кого они находятся, производится их выемка



Порядок выемки соответствует порядку производства обыска, предусмотренному ст. 182 УПК РФ. Вместе с тем, выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, а также вещей, заложенных или сданных на хранение в ломбард, производится на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ.

На основании судебного решения, также производится выемка медицинских документов, содержащих сведения о наличии у гражданина психического расстройства, о фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья, являющиеся врачебной тайной



О производстве выемки составляется протокол, форма и содержание которого идентичны с протоколом обыска.

Лицо, получившее копию протокола, дает об этом расписку.

В случае выемки заложенной или сданной на хранение в ломбард вещи в трехдневный срок производится уведомление об этом заемщика или поклажедателя

3. Назначение и производство предварительных исследований или судебных экспертиз.

В ходе раскрытия и расследования хищений денежных средств в системе ДБО в зависимости от возникшей оперативно-розыскной и следственной ситуации могут проводиться различные виды предварительных исследований и судебных экспертиз. Они могут быть разными, но в научной литературе их называют судебными компьютерно-техническими экспертизами, которые подразделяют на:

- аппаратно-компьютерные;
- программно-компьютерные;
- информационно-компьютерные;
- компьютерно-сетевые.

Однако во всех случаях при производстве перечисленных видов исследований или экспертиз объектом исследования будет являться компьютерная информация. Она может быть в виде дампа памяти; дампа сетевого трафика; журналов регистрации событий от интернет-провайдера; журналов регистрации событий кредитной организации, предоставляющей

систему ДБО; операционной системы; программного обеспечения комплектующих и периферийных устройств; прикладных программ; различной вспомогательной компьютерной информации, необходимой для их функционирования; различных баз данных, представленных в форматах, обеспечивающих автоматизированное хранение, поиск, обработку и передачу и т.д.

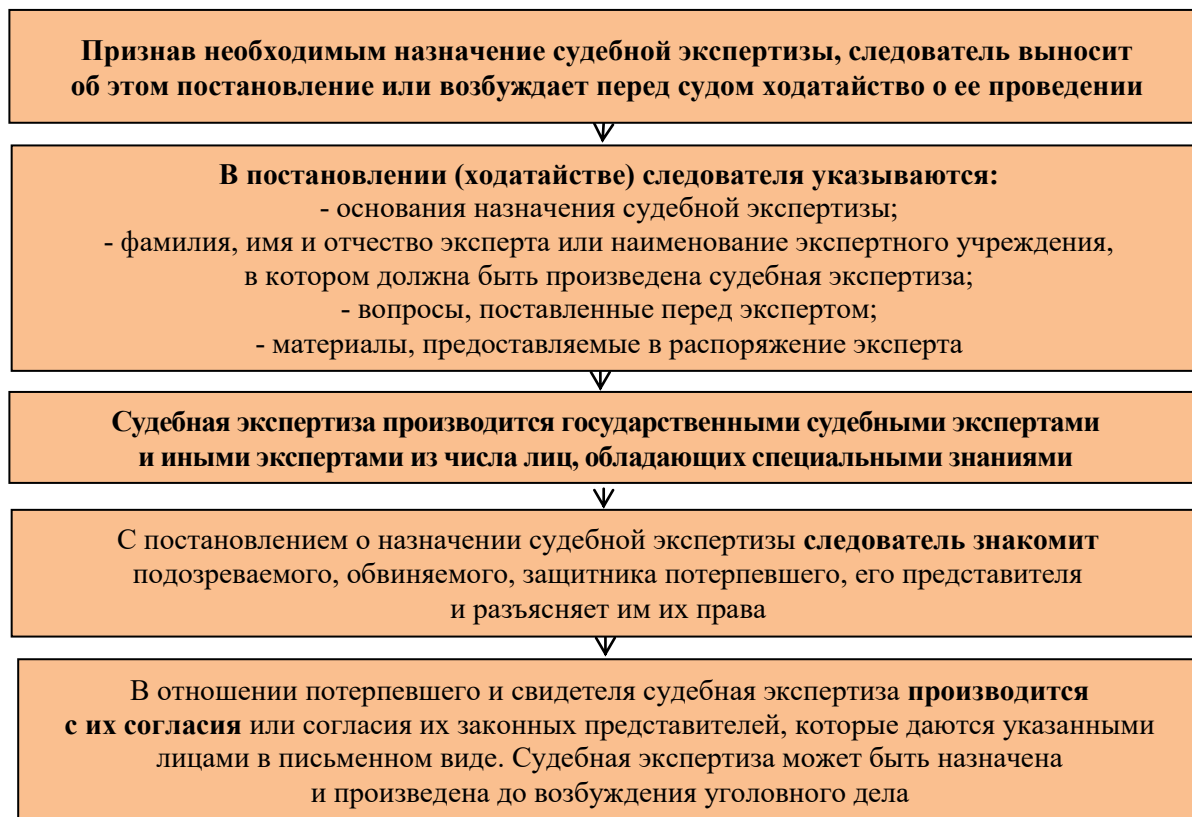
В ходе производства исследования или судебной экспертизы по хищениям денежных средств, совершаемых в системе ДБО, ключевыми вопросами, подлежащими выяснению, являются:

- установление способа хищения и определения способа доступа к компьютеру потерпевшего;
- установление сведений о лице (-ах), причастном (-ых) к хищению денежных средств, а также определение роли каждого участника;
- каким способом осуществлялось списывание денежных средств со счета потерпевшего в системе ДБО.

Предлагаем рассмотреть схему «Порядок назначения судебной экспертизы» согласно нормам ст. 195 УПК РФ²⁷ (см. схему 4).

²⁷ Шаталов А.С. Указ. раб. – С. 340.

Порядок назначения судебной экспертизы (ст. 195 УПК РФ)



4. Допрос.

Как нам известно, в природе раскрытия и расследования подготавливаемых или уже совершенных преступлений не существует ни одного уголовного дела, в расследовании которого не было проведено хотя бы одного допроса.

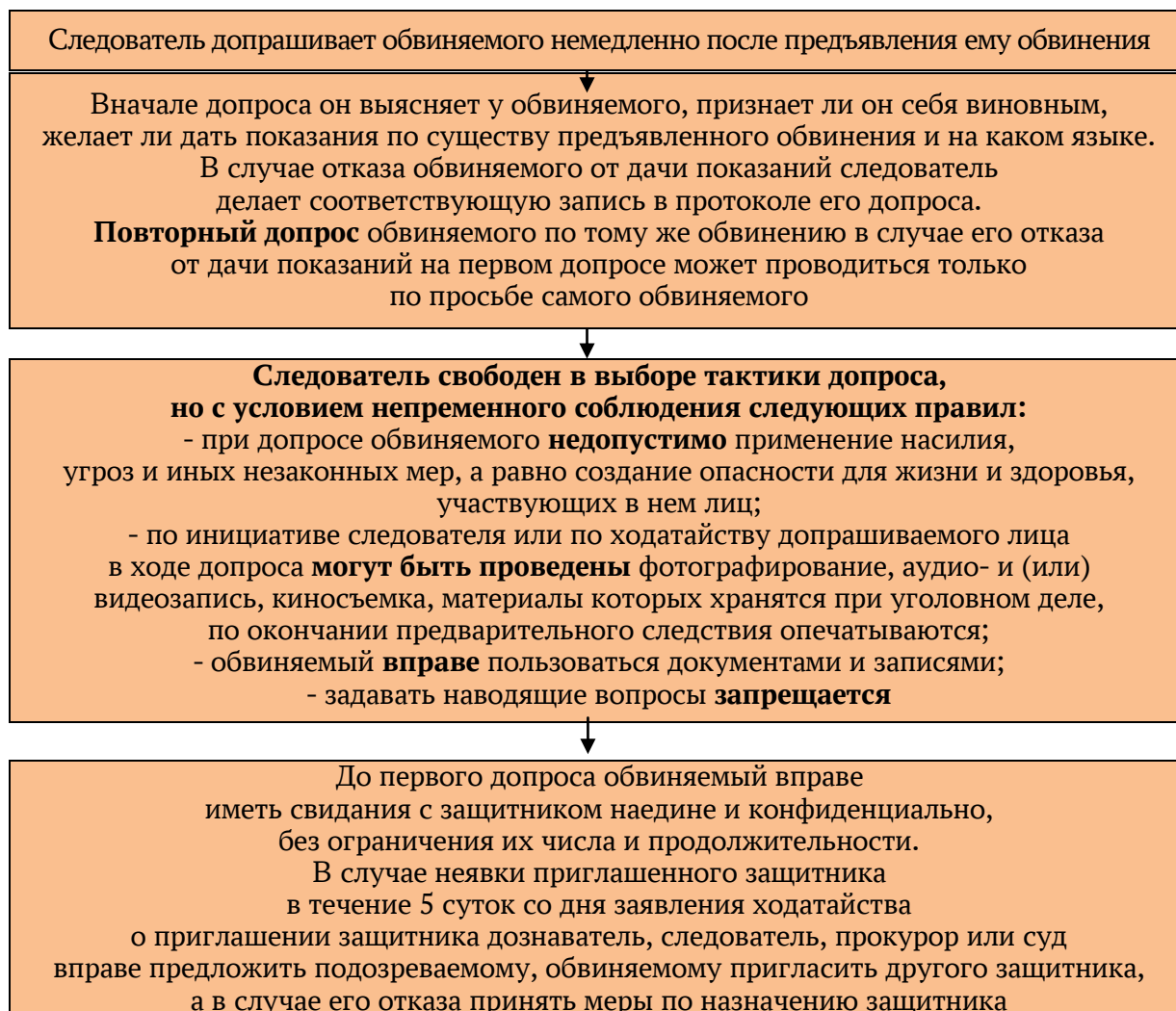
Предлагаем ознакомиться с классической схемой допроса обвиняемого (см. схему 5). Протокол допроса обвиняемого согласно нормам ст. 174 УПК РФ должен быть оформлен следующим образом:

1. При каждом допросе обвиняемого следователь составляет протокол с соблюдением требований ст. 190 УПК РФ.

2. В протоколе первого допроса указываются данные о личности обвиняемого:

- 1) фамилия, имя и отчество;
- 2) дата и место рождения;
- 3) гражданство;
- 4) образование;
- 5) семейное положение, состав его семьи;
- 6) место работы или учебы, род занятий или должность;
- 7) место жительства;
- 8) наличие судимости;
- 9) иные сведения, имеющие значение для уголовного дела.

Допрос обвиняемого (ст. 173 УПК РФ)²⁸



3. В протоколах следующих допросов данные о личности обвиняемого, если они не изменились, можно ограничить указанием его фамилии, имени и отчества.

После ознакомления с необходимыми следственными действиями и представленными схемами полагаем перейти к тактике осуществления допроса применимо к расследованию уголовных дел по факту хищения денежных средств, совершаемых в системе ДБО.

Все виды допросов (потерпевшего, свидетеля, подозреваемого, обвиняемого) согласно существующим разработанным положениям науки криминалистики осуществляются с использованием тактических рекомендаций²⁹.

²⁸ Шаталов А.С. Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие. Москва: Проспект, 2021. С. 300.

Каждый из них нацелен на получение полных и правдивых показаний относительно событий, имеющих отношение к расследуемому уголовному делу. Они связаны с получением вербальной (то есть словесной) информации, интересующей следствие.

При их производстве следователь познает события, получая доказательства опосредствованно – путем передачи ему сведений другими лицами, ранее воспринимавшими те или иные факты, явления, действия³⁰.

Основание и его производство урегулированы статьями 187-191 УПК РФ. Данное следственное действие по праву считается наиболее распространенным. Довольно редко возникает острая потребность в проведении следственных экспериментов. Что касается допроса, то можно безошибочно предположить, что в истории уголовного судопроизводства, пожалуй, не было ни одного расследованного уголовного дела, по которому он вообще не производился.

Допрос осуществляется по месту производства предварительного следствия.

В зависимости от складывающейся ситуации следователь вправе, если считает это необходимым, провести допрос в месте нахождения допрашиваемого (например, в жилище, по месту работы, в следственном изоляторе).

Допрос не может длиться более 4 часов. Его продолжение законом допускается после перерыва для отдыха и принятия пищи. Длительность такого перерыва составляет не менее одного часа, а общая продолжительность допроса в течение дня не должна превышать 8 часов. **Наводящие вопросы допрашиваемому лицу задавать запрещается.**

В остальном следователь свободен в выборе тактики допроса. Допрос проводится без понятий. Ход и результаты данного следственного действия отражаются в протоколе, составленном в соответствии со ст. 166 и 167 УПК РФ.

Как известно, в ходе расследования уголовных дел по факту хищений денежных средств, совершенных в системе ДБО, возникают различные следственные ситуации.

В зависимости от возникшей обстановки для выяснения спорных и возникающих вопросов в процессе производства допросов потерпевшего и лиц, имеющих возможность доступа к компьютеру, на котором установлена система ДБО, необходимо уточнить следующее:

- кто интересовался программным обеспечением, установленным на компьютер потерпевшего;

²⁹ Криминалистика. Полный курс: учебник для вузов / под общ. ред. А.Г. Филиппова. С. 417.

³⁰ Шаталов А.С., Крымов А.А. Уголовно-процессуальное право Российской Федерации: академический курс по направлению «Юриспруденция». М.: Проспект, 2018.

- в помещении, где расположен компьютер, были ли когда-либо посторонние лица;
- были ли в данном помещении посторонние лица, работающие на проверяемом компьютере и не имеющие доступа к нему;
- не зафиксированы ли случаи работы кого-либо из лиц, имеющих доступ к компьютеру, с информацией, не относящейся к их компетенции;
- как часто проверялись установленные программы на наличие вирусов, и каковы были их результаты, в частности, последних проверок;
- каким путем и где приобретались проверочные программы на наличие и устранение вирусов;
- были ли зафиксированы сбои в работе компьютерного оборудования, электронных сетей и средств защиты компьютерной информации;
- имели ли место случаи неправомерного доступа к компьютерной информации ранее, если да, то, как часто;
- кто еще подключен к компьютерной сети и является ее абонентом;
- каким образом осуществляется защита компьютерной информации, какие при этом средства и методы защиты применяются;
- как Вы считаете, могло ли случайно произойти списание денежных средств с банковского счета (результат Вашего неосторожного действия или неисправности работы компьютерной системы или сбоев программного обеспечения);
- были ли такие факты, как отстранение от работы лиц, имевших доступ к компьютеру потерпевшего и в том числе в результате увольнения в течение интересующего периода, и по каким мотивам.

Таблица 1

**Оперативно-розыскные мероприятия
и первоначальные следственные действия**

№ п/п	<i>Оперативно-розыскные мероприятия и первоначальные следственные действия</i>	<i>Подразделения ОВД, ответственные за проведение указан- ных действий и мероприятий</i>
1	Незамедлительное информирование дежурной части УМВД России по г. Энску о зарегистрированных фактах хищения денежных средств, совершенных с использованием средств мобильной (стационарной связи). Организация своевременного выезда следственно-оперативной группы (СОГ) на место происшествия	<i>Дежурная часть территориального ОВД</i>
2	<i>Мероприятия, осуществляемые сотрудниками отдела уголовного розыска (ОУР):</i> 1) опрос заявителя (получение информации об абонентских номерах, номерах банковских карт, интернет-страницах, используемых преступниками, с указанием точного времени поступления звонка, если звонок потерпевшим поступил на стационарный телефон, необходимо отобрать у владельца заявление с исчерпывающей информацией; 2) предоставление полученной информации дежурному сотруднику Управления уголовного розыска (УУР), ПСТМ, Управления экономической безопасности и противодействия коррупции (УЭБиПК) УМВД России по Энской области; 3) принятие мер к получению детализации по абонентскому номеру потерпевшего, на который поступил звонок (через Интернет, отделение операторов связи совместно с потерпевшим), получению выписки по карте (через отделения банков по заявлению потерпевшего), сведений об интернет-страницах (приобщению копий страниц к материалу проверки), чеков денежных перечислений; 4) при получении новых сведений сотрудники, ответственные за формирование информационно-поисковой системы (ИПС), осуществляют ввод информации в базу данных (БД) и ее корректировку	<i>СОГ территор. ОВД</i>
3	<i>Мероприятия, осуществляемые сотрудниками следственного отдела (СО) и отдела дознания (ОД):</i> 1) Осмотр места происшествия, аппарата сотовой связи, компьютерной техники, банкоматов, терминалов оплаты; изъятие документов, подтверждающих информацию о переводах денежных средств;	<i>СО, ОД</i>

	2) Принятие решения по обращению заявителя в порядке статей 144-145 УПК РФ; 3) Допрос заявителей, свидетелей; 4) При установлении факта незаконного списания денежных средств неустановленным способом изъять сотовый телефон (без SIM-карты) потерпевшего для направления в ЭКЦ УМВД России по Энской области для проведения компьютерной экспертизы. <i>В рамках возбужденного уголовного дела в течение суток следователю необходимо:</i> а) вынести ходатайства перед судом: - о получении информации о соединениях между абонентами и (или) абонентскими устройствами; - о получении информации о движении денежных средств по расчетному банковскому счету потерпевшего, балансу абонентского номера телефона, месте фактического нахождения сотовых телефонов злоумышленников; - о наложении арестов на расчетные счета/виртуальные счета SIM-карт злоумышленников; - на проведение соответствующих ОРМ по абонентским и IMEI-номерам преступников (при необходимости); б) запросить информацию в кредитных организациях (банках) операторов сотовой связи, электронных платежных системах: - сведения о движении денежных средств по счетам (банковским картам) потерпевшего и преступника; - сведения о принадлежности абонентских номеров, используемых преступником; - сведения о виртуальных счетах (регистрационные данные, электронное администрирование, движение денежных средств); в) при установлении места нахождения собственников SIM-карт и банковских карт направить поручение в соответствующие органы для полноты установления фактических обстоятельств совершенного преступления. 5) При получении новых сведений сотрудники, ответственные за формирование ИПС, осуществляют ввод информации в БД и ее корректировку. 6) Своевременное внесение необходимой информации в базу Информационного центра (ИЦ) УМВД «Дистанционные Преступления» (по примеру Энской области)	
4	<i>Мероприятия, осуществляемые сотрудниками ПСТМ МВД России:</i> 1) принять неотложные меры для оперативного получения информации об имеющихся абонентских номерах, принадлежности банковских карт (счетов), используемых злоумышленниками; движении по ним денежных средств и	<i>ПСТМ МВД России</i>

	местах их обналичивания (номера и адреса банкоматов); при возможности использования сервисов ДБО карты потерпевшего; детализации телефонных соединений по стационарному номеру потерпевшего, во взаимодействии с ПАО «Ростелеком»; 2) подготовить постановление о приостановлении услуг связи по установленным абонентским номерам; 3) подготовить информационное письмо в Роскомнадзор, если абонентский номер реализован без внесения сведений об абоненте или реализован с внесением недостоверных данных об абоненте; 4) передать полученную информацию дежурному сотруднику УУР, СУ, ОД УМВД; 5) При получении новых сведений сотрудники, ответственные за формирование ИПС, осуществляют ввод информации в БД и ее корректировку	
5	<i>Мероприятия, проводимые Следственным управлением (СУ), ОД:</i> - осуществлять взаимодействие с территориальными СОГ. При необходимости осуществить выезд на место происшествия. Обеспечивать контроль за квалификацией возбужденных уголовных дел, качеством проведения следственных действий и полученных результатов, подготовкой ходатайств и получением судебных решений по установленным абонентским номерам; - подготавливать необходимые запросы в банки или иные кредитные организации. Проводить контроль за предоставлением соответствующих реквизитов в статистических карточках по форме 1, заполнить реквизит № 26 согласно справочнику 12, где указать способ совершения преступления (49,50), при использовании мошенниками сети Интернет заполнить реквизит 28, указав значение 100 и 037; - ИПК-ПР (Л), кроме основной информации заполнить способ мошенничества/кражи (реквизит 51 с указанием значения 20 (сотового телефона)	СУ, ОД
6	<i>Мероприятия, осуществляемые Управлением уголовного розыска (УУР), отделом оперативно-розыскной информации (ООРИ) БСТМ МВД России:</i> осуществить контроль за проведением ОРМ и получить сведения из территориальных ОВД об абонентских номерах, банковских картах (счетах), используемых злоумышленниками, предоставить информацию дежурному сотруднику ПСТМ и УЭБиПК УМВД России по Энской области; при получении информации от сотрудника ПСТМ, ООРИ осуществить проверку установленных владельцев абонентских номеров и банковских карт (счетов) по учетам информационной системы (ИС) оперативно-розыскной информации (ОРИ); полученную информацию предоставить дежурному сотруднику ОУР территориального ОВД для дальнейшего приобщения к материалам уголовного дела	УУР, ООРИ БСТМ МВД России

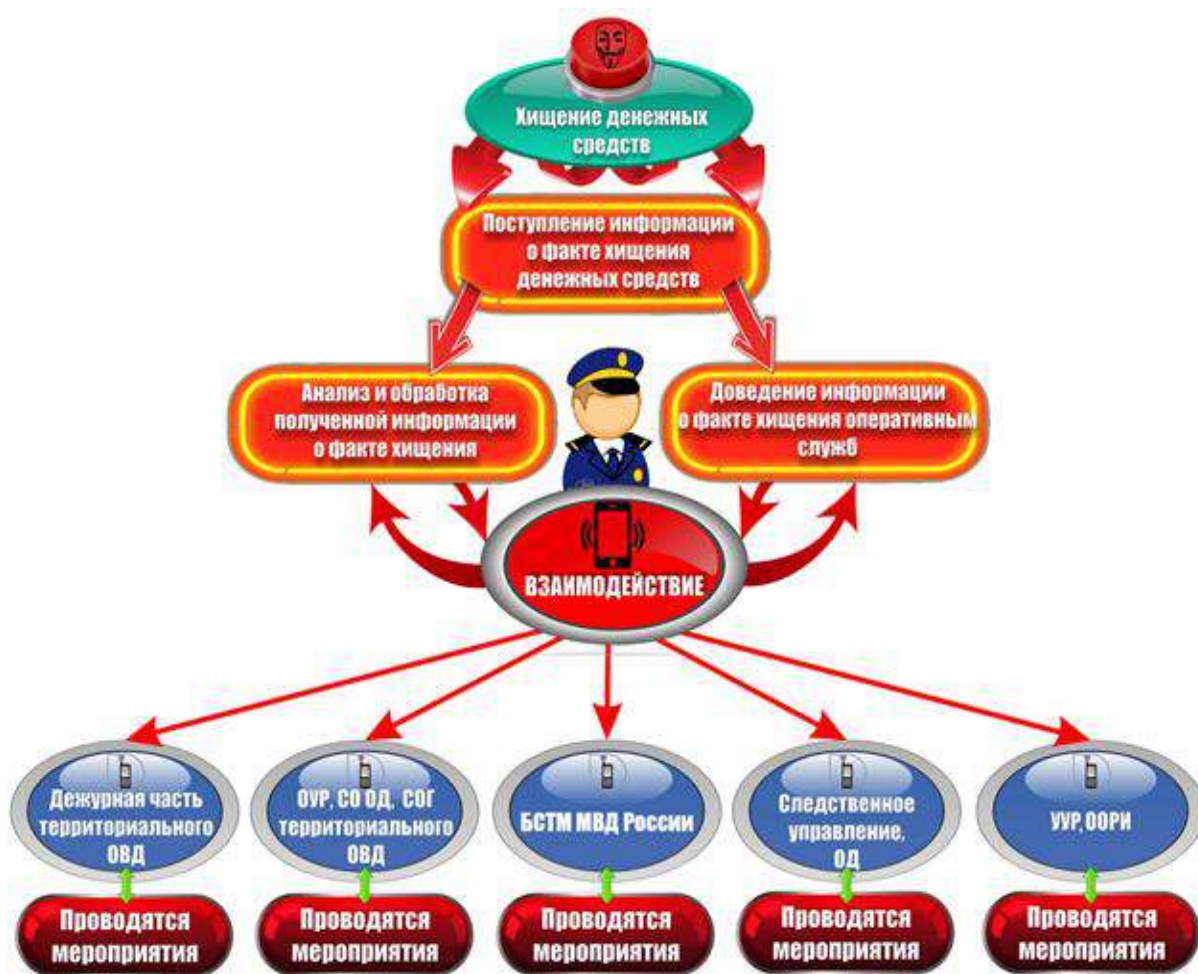


Рис. 15. Схема взаимодействия

4.5. Профилактика хищений денежных средств в системе дистанционного банковского обслуживания

В целях повышения эффективности проводимых мероприятий по предупреждению и раскрытию хищений денежных средств граждан, совершаемых с использованием средств ДБО и мобильной связи, считаем необходимым:

1. Во взаимодействии со следственными подразделениями, судебными органами и прокуратурой региона необходимо разработать проект постановления о возбуждении перед судом ходатайства на проведение оперативно-розыскных мероприятий в виде наведения справок и судебных постановлений, позволяющих получить у представителей операторов связи информацию:

- принадлежность абонентского номера;

- географическое положение аппарата связи, в котором установлена и эксплуатировалась SIM-карта с абонентским номером в интересующий период времени;

- детализацию входящих и исходящих телефонных соединений за интересующий период времени; IMEI-номерах, с которыми эксплуатировалась SIM-карта;

- поступление и списание денежных средств по счету абонентского номера.

2. На базе информационных подразделений необходимо создать единый информационный банк данных указанных преступлений, в котором отражать сведения:

- о потерпевшем;
- о способе хищения денежных средств;
- об абонентских номерах;
- об электронных и банковских счетах.

3. Организовать своевременный взаимообмен информацией с региональными подразделениями УМВД России.

4. На законодательном уровне установить и ограничить сроки исполнения запросов операторам связи, провайдерам и банковским структурам, путем наделения территориальных представителей правами доступа к общим базам данных, установление ответственности за ненадлежащее исполнение, а также вменить в обязанность проведение профилактических мероприятий в адрес клиентов.

5. Постоянно осуществлять профилактическую работу по надежному обеспечению безопасного предоставления услуг дистанционного (удаленного) обслуживания (например, программное обеспечение или определенные алгоритмы) и, в случае совершения хищений, обязать банки и платежные системы возвращать клиентам денежные средства.

6. Согласовать работу определенного рода, направленную на незамедлительное получение информации о совершенных фактах нарушений и преступлений в системе ДБО за конкретный период времени. Исходя из полученных сведений о складывающейся ситуации, осуществлять глубокий анализ криминогенной обстановки и вносить корректировку в действующую систему ДБО населения.

7. Проработать вопрос о расширении страховых услуг денежных средств, находящихся на счетах клиентов организаций, оказывающих банковские услуги.

8. Размещать информацию о фактах мошеннических действий, совершенных с использованием аппаратов сотовой связи (стикеры, баннеры), в организациях, осуществляющих работу с гражданами (РЭУ, пенсионные фонды, дома культуры, органы соцзащиты и т.д.), на объектах

общего пользования (отделения банков, магазины, торговые центры, кафе и т.д.). Данные профилактические мероприятия должны носить в зависимости от возникшей ситуации «адресный» характер и охватывать все слои населения, включая наиболее уязвимые группы.

9. Зональным оперативным сотрудникам, обеспечивающим безопасность дистанционного банковского обслуживания населения, проводить на закрепленных административных участках профилактическую работу, направленную на подробное разъяснение современных способов совершения преступлений, связанных с хищением денежных средств в системе ДБО.

10. Доведение информации гражданам через сотрудников банков о необходимости разъяснения своим клиентам сведений о совершаемых мошенничествах с использованием аппаратов сотовой связи и банковских карт.

11. Постоянно осуществлять размещение статей во всевозможных печатных изданиях и Интернете о современных способах мошенничества и других видов преступлений, связанных с дистанционным банковским обслуживанием и совершенных с использованием аппаратов сотовой связи и банковских карт.

Глава V. Обзор преступлений, совершенных в условиях цифровизации

В связи с интенсивным развитием информационных технологий, средств связи, банковских услуг, в том числе электронных платежей и внедрением их в повседневную жизнь происходит адаптация схем преступных деяний, направленных на завладение денежными средствами граждан. Наиболее распространенными являются мошеннические действия, совершенные с использованием средств проводной и сотовой связи.

Рассмотрим пример из Н-ской области.

По результатам проведенного анализа материалов возбужденных уголовных дел (совместно с УМВД и СУ УМВД) установлено, что в 2025 году на территории Н-ской области было зарегистрировано 792 факта хищения денежных средств мошенническим путем с использованием средств проводной, сотовой связи и сети Интернет.

Наиболее распространенными схемами являются:

- вредоносное программное обеспечение телефонного аппарата на операционной системе «Android» (129 фактов – 16%);
- получение звонков, SMS-сообщений «Ваша карта заблокирована» (118 фактов – 15%);
- размещение объявления в сети Интернет (потерпевший/преступник) (395 фактов – 50%);
- ложная информация – компенсация за «БАДы», «Молитвы», «Экстрасенсы», «Бонусы к пенсии» (47 фактов – менее 6%);
- преступник из окружения потерпевшего получил доступ к карте или потерпевший потерял карту (13 фактов – менее 2%).

Проанализировав ежемесячные сборники «Состояния преступности в России за 2025 год» определены регионы с наибольшими темпами прироста зарегистрированных преступлений, в %:

- Ненецкий АО – 154,2;
- Республика Калмыкия – 74,7;
- Новгородская область – 71,5;
- Калининградская область – 63,8;
- Республика Ингушетия – 62,2;
- г. Севастополь – 61,4;
- Липецкая область – 58,7;
- Новосибирская область – 51,9;
- Республика Башкортостан – 49,2;
- Республика Хакасия – 48,8.

Для более наглядного и глубокого понимания складывающейся криминогенной обстановки на территории Российской Федерации приводим сводные данные о преступлениях, совершенных в системе дистанционного банковского обслуживания с использованием компьютерных технологий.

Таблица 2

**Динамика краж, совершенных с использованием
компьютерных технологий на территории Российской Федерации
с 2018 по 2023 гг.**

Годы	Количество краж, уголовные дела о которых находились в производстве	В том числе количество преступлений			
		Количество краж, зарегистрированных в отчетном периоде	Из них выявлено сотрудниками подразделений СТМ	По которым установлены лица сотрудниками подразделений СТМ	Уголовные дела, о которых прекращены по реабилитирующим основаниям
2018	2681	2015	1292	912	78
2019	4173	3891	2994	1512	133
2020	4357	4120	3821	1912	175
2021	4576	4496	4217	2311	190
2022	4715	4832	4678	2700	199
2023	4819	4952	4715	2792	212

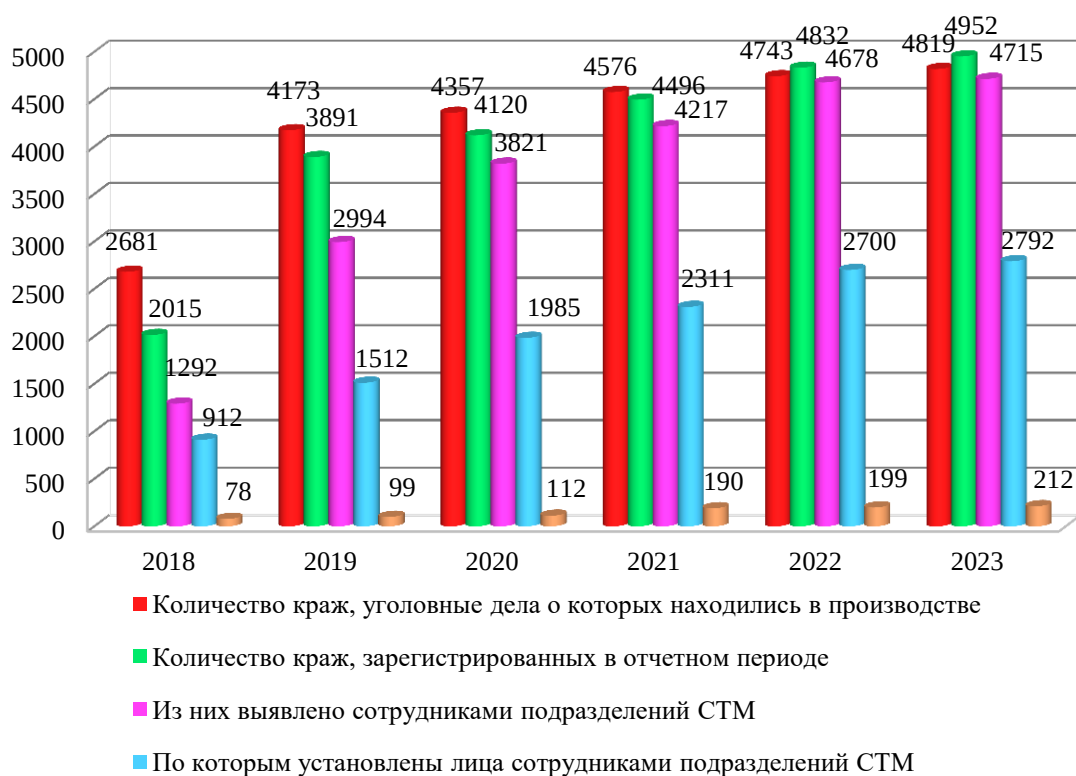


Диаграмма 2. Динамика краж, совершенных с использованием компьютерных технологий на территории России с 2018 по 2023 гг.

Таблица 3

**Динамика краж, в том числе количество преступлений
с использованием компьютерных технологий, и движение уголовных дел**

Годы	В том числе количество преступлений, уголовные дела о которых				
	Закончены расследованием либо разрешены в отчетном периоде	Из них		Приостановлены за нерозыском лица либо в случае неустановления лица, совершившего преступление	Из них должностными лицами ОПС ОВД
		Направлено в суд	В том числе должностными лицами ОПС ОВД		
2018	1341	1008	998	1157	772
2019	2035	1234	1176	1287	912
2020	1985	1347	1311	1395	953
2021	2376	1543	1573	1531	1023
2022	2870	1854	1895	1734	1123
2023	3251	3125	2732	1828	1237

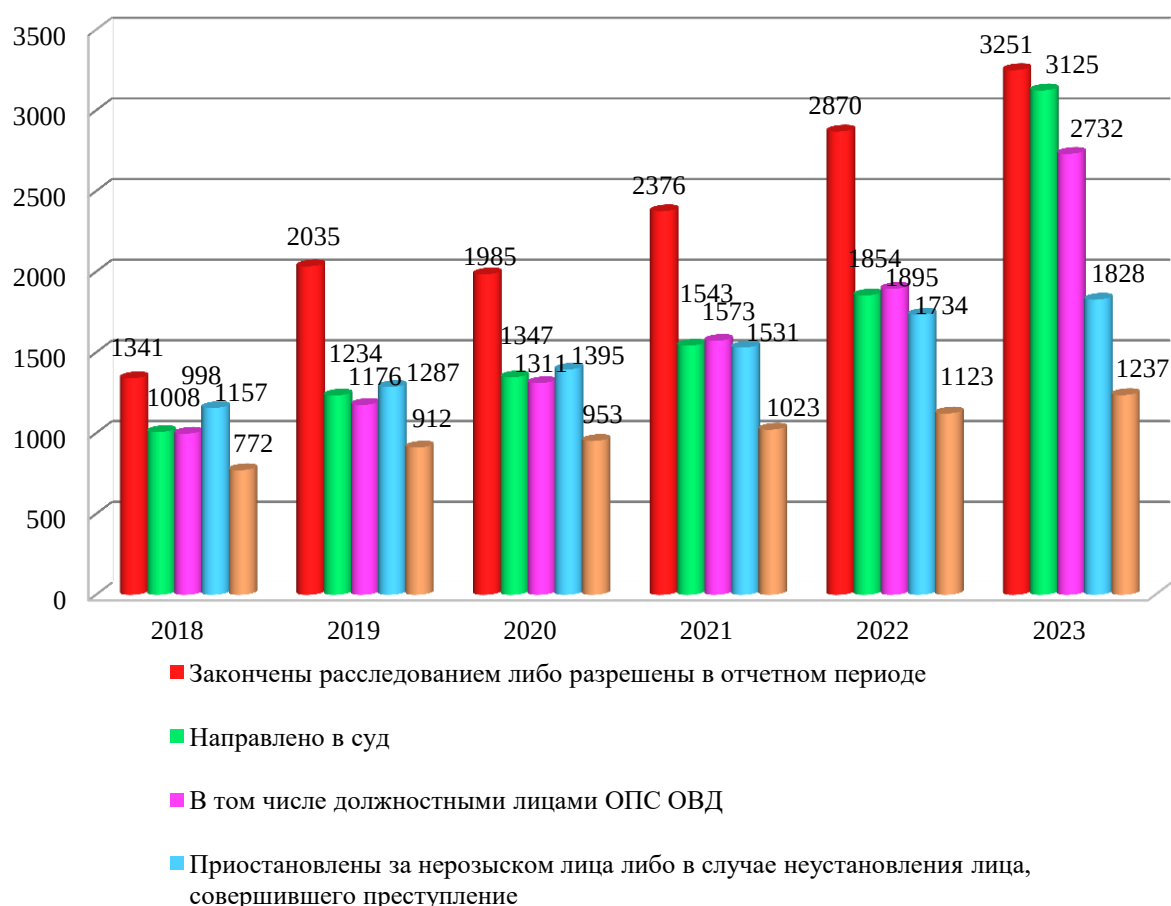


*Диаграмма 3. Динамика краж, в том числе количество преступлений
с использованием компьютерных технологий, и движение уголовных дел*

На представленной ниже диаграмме видно, какой процент от общего количества уголовных дел, по которым лица, совершившие преступления, установлены сотрудниками подразделений СТМ, составляют уголовные дела, прекращенные по реабилитирующим основаниям. Таким образом, из этого следует, что в более чем в 90% случаев выявленные сотрудниками ПСТМ и подозреваемые в совершении преступлений лица в последующем несут наказание, соответствующее нормам уголовно-процессуального законодательства (см. диаграмму 4).

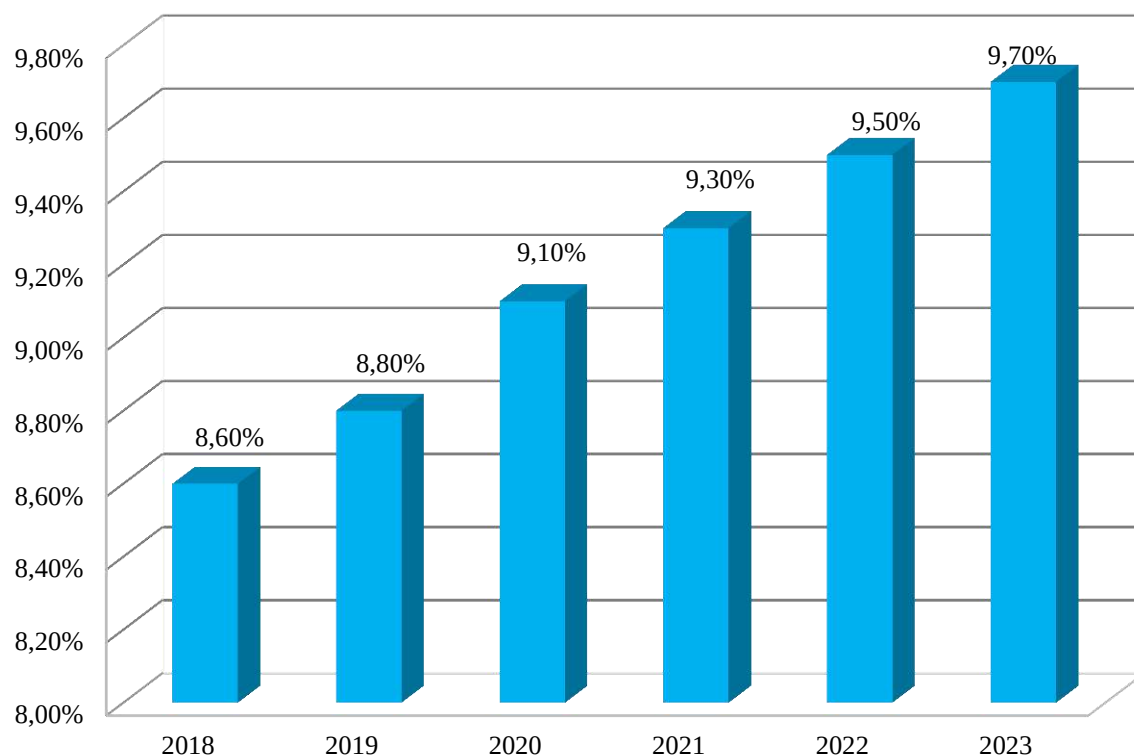


Диаграмма 4. Удельный вес уголовных дел, прекращенных по реабилитирующим основаниям³¹ %

³¹ Из числа дел, по которым лица, совершившие преступления данной категории на территории Российской Федерации, установлены сотрудниками подразделений СТМ в 2018-2023 гг.

Таблица 4

Динамика уголовных дел в 2018-2023 гг.

Годы	Количество краж, уголовные дела о которых находились в производстве	Закончены расследованием либо разрешены в отчетном периоде	Направлено в суд	Приостановлены за нерозыском лица, либо в случае неустановления лица, совершившего преступление
2018	2681	1341	1008	1157
2019	4173	2035	1234	1287
2020	4357	1985	1347	1395
2021	4412	2175	1586	1486
2022	4715	2215	1624	1599
2023	4819	2384	1764	715

Из следующей диаграммы видно, что количество краж с использованием компьютерных технологий с каждым годом увеличивается.



Диаграмма 5. Динамика уголовных дел в 2018-2023 гг.

Таблица 5

Удельный вес уголовных дел в 2018-2023 гг., %

Год	Количество краж, уголовные дела о которых находились в производстве	Закончены расследованием либо разрешены в отчетном периоде		Приостановлены за нерозыском лица, либо в случае неустановления лица, совершившего преступление	
		Количество	Удельный вес	Количество	Удельный вес
2018	2681	1341	50,01%	1157	43,15%
2019	4173	2035	48,76%	1287	30,84%
2020	4357	1985	45,55%	1395	32,00%
2021	4412	2175	49,29%	1486	33,68%
2022	4715	2215	46,97%	1599	33,91%
2023	4819	2376	45,86%	1583	33,64%

На диаграмме ниже видно, что количество уголовных дел, законченных расследованием либо разрешенных в отчетном периоде, составляет примерно половину от всех уголовных дел, находящихся в производстве. Количество приостановленных за нерозыском лица, либо в случае неустановления лица, совершившего преступление, составляет около одной трети от всех уголовных дел, находящихся в производстве (диаграмма 6).



Диаграмма 6. Удельный вес уголовных дел в 2018-2023 гг., %

Таблица 6

**Динамика мошенничеств (ст. 159 УК), совершенных
с использованием компьютерных технологий на территории
Российской Федерации в 2010-2023 гг.**

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	в том числе количество преступлений			
		количество мошенничеств, зарегистриро- ванных в от- четном перио- де	из них	по которым установлены лица сотру- дниками под- разделений СТМ	уголовные де- ла, о которых прекращены по реабилитиру- ющим основа- ниям
			выявлено со- трудниками подразделений СТМ		
2010	1199	1010	537	190	127
2011	1819	1527	910	582	85
2012	2049	1805	1319	672	99
2013	3148	2748	1399	508	195
2014	2805	2196	1033	459	457
2015	2917	2071	1180	525	402
2016	3058	2172	1238	550	357
2017	3189	2265	1291	574	426
2018	3274	2325	1325	589	548
2019	3356	2475	1399	631	656
2020	3920	2520	1498	689	654
2021	4095	2749	1725	748	709
2022	4207	3061	2099	890	802
2023	4295	3123	2157	902	839

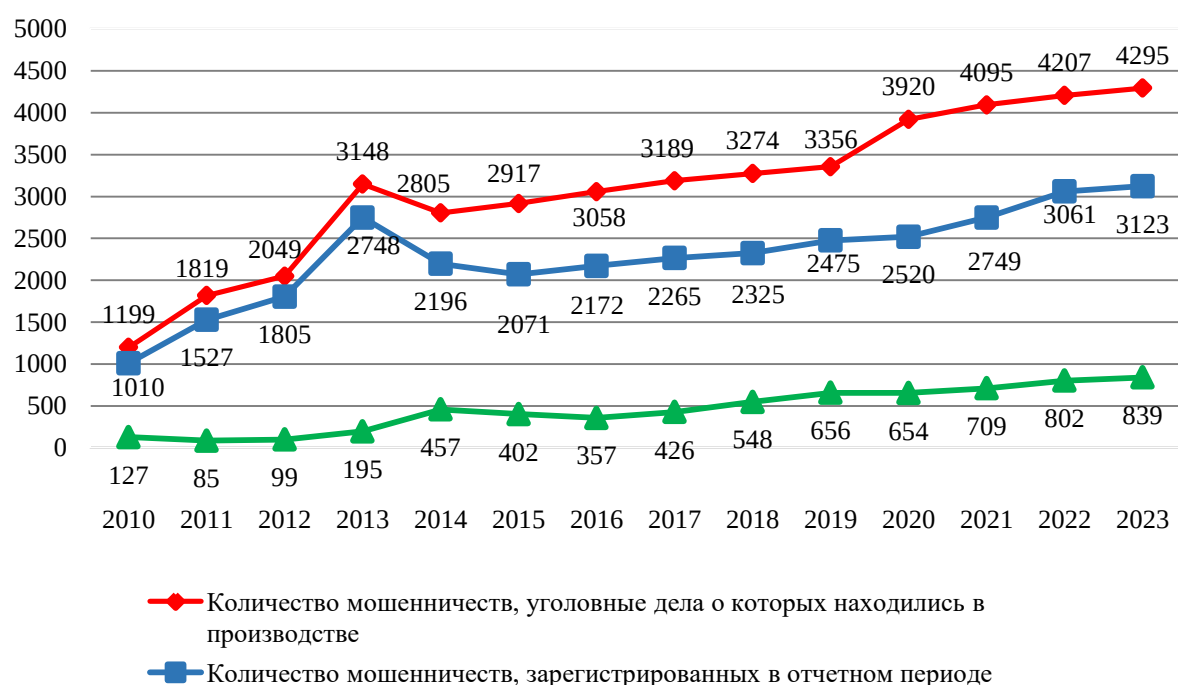


Диаграмма 7. Динамика мошенничеств (ст. 159 УК), совершенных с использованием компьютерных технологий на территории Российской Федерации в 2010-2023 гг.

**Динамика мошенничеств
с использованием компьютерных технологий
и движение уголовных дел в 2010-2023 гг.**

Годы	в том числе количество преступлений, уголовные дела о которых				
	Закончены рас- следованием либо разрешены в отчетном периоде	из них		приостановлены за нерозыском лица либо в случае неуста- новления лица, совершившего преступление	из них должност- ными лица- ми ОПС ОВД
		направлено в суд	в том числе должностными лицами ОПС ОВД		
2010	611	597	513	329	290
2011	1019	998	865	404	338
2012	972	957	903	630	504
2013	1333	1255	1134	1113	855
2014	782	665	592	1318	1085
2015	1420	1302	1152	1567	1345
2016	1123	1045	985	1754	1568
2017	987	846	749	1967	1754
2018	1210	1096	957	2015	1865
2019	1513	1421	1233	2312	2001
2020	1690	1602	1403	2659	2530
2021	1740	1700	1590	2896	2750
2022	1820	1799	1620	3044	2902
2023	2067	1958	1854	2964	2973

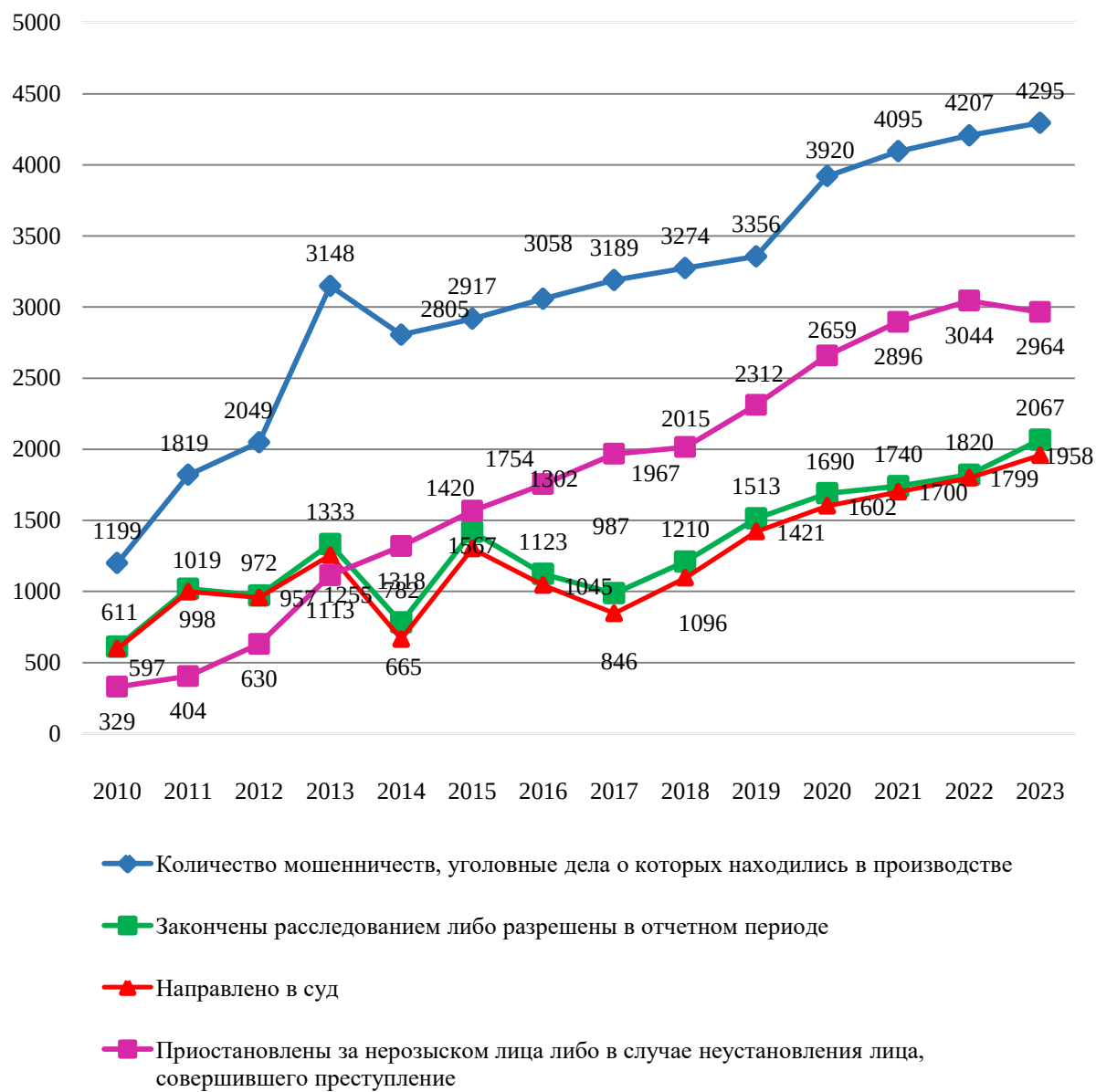


Диаграмма 8. Динамика преступлений в 2010-2023 гг.

Таблица 8

**Удельный вес мошенничеств
с использованием компьютерных технологий в 2010-2023 гг., %**

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Выявлено сотрудниками подразделений СТМ	
		Количество	Удельный вес
2010	1199	537	44,8%
2011	1819	910	50,0%
2012	2049	1319	64,4%
2013	3148	1399	44,4%
2014	2805	1033	36,8%
2015	2917	1180	40,5%
2016	3058	1238	40,5%
2017	3189	1291	40,5%
2018	3274	1325	40,5%
2019	3356	1399	41,6%
2020	3920	1498	38,2%
2021	4095	1725	42,1%
2022	4207	2099	49,9%
2023	4295	2332	54,3%

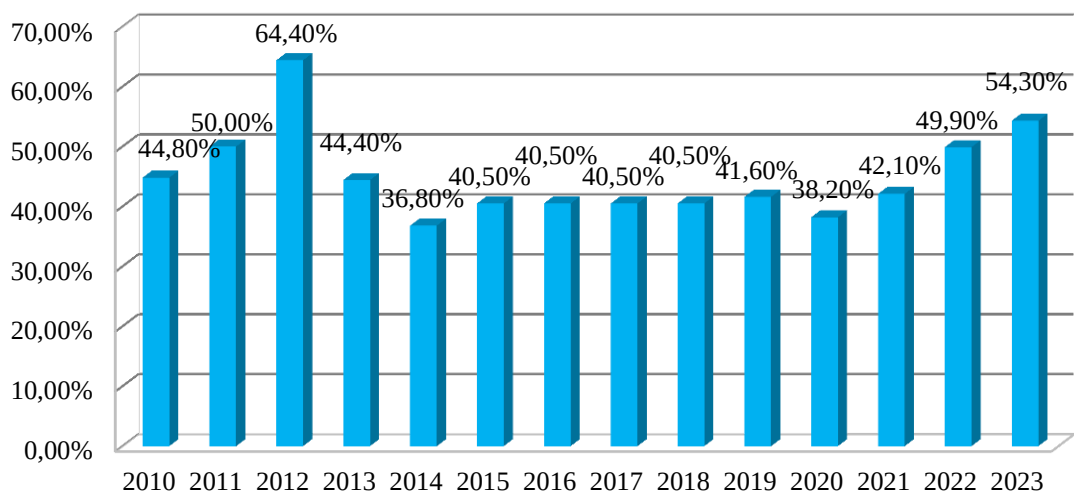
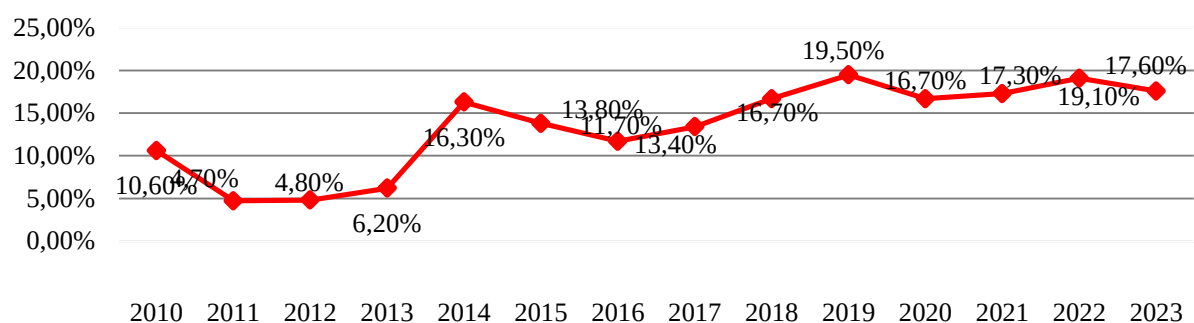


Диаграмма 9. Удельный вес мошенничеств с использованием компьютерных технологий в 2010-2023 гг., %

Таблица 9

**Удельный вес прекращенных уголовных дел
по реабилитирующим основаниям в 2010-2023 гг., %**

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Уголовные дела, прекращенные по реабилитирующим основаниям	
		Количество	Удельный вес
2010	1199	127	10,6%
2011	1819	85	4,7%
2012	2049	99	4,8%
2013	3148	195	6,2%
2014	2805	457	16,3%
2015	2917	402	13,8%
2016	3058	357	11,7%
2017	3189	426	13,4%
2018	3274	548	16,7%
2019	3356	656	19,5%
2020	3920	654	16,7%
2021	4095	709	17,3%
2022	4207	802	19,1%
2023	4295	755	17,6%



—♦— Уголовные дела, прекращенные по реабилитирующим основаниям

Диаграмма 10. Удельный вес прекращенных уголовных дел по реабилитирующим основаниям в 2010-2023 гг, %

Таблица 10

Удельный вес уголовных дел в 2010-2023 гг., в %

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Закончены расследованием либо разрешены в отчетном периоде		Приостановлены за нерозыском лица либо в случае неустановления лица, совершившего преступление	
		Количество	Удельный вес	Количество	Удельный вес
2010	1199	611	51,0%	329	27,4%
2011	1819	1019	56,0%	404	22,2%
2012	2049	972	47,4%	630	30,7%
2013	3148	1333	42,3%	1113	35,4%
2014	2805	782	27,9%	1318	47,0%
2015	2917	1420	48,7%	1567	53,7%
2016	3058	1123	36,7%	1754	57,4%
2017	3189	987	31,0%	1967	61,7%
2018	3274	1210	37,0%	2015	61,5%
2019	3356	1513	45,0%	2312	68,8%
2020	3920	1690	43,1%	2659	67,8%
2021	4095	1740	42,5%	2896	70,7%
2022	4207	1820	43,3%	3044	72,4%
2023	4295	2067	48,1%	2964	69%

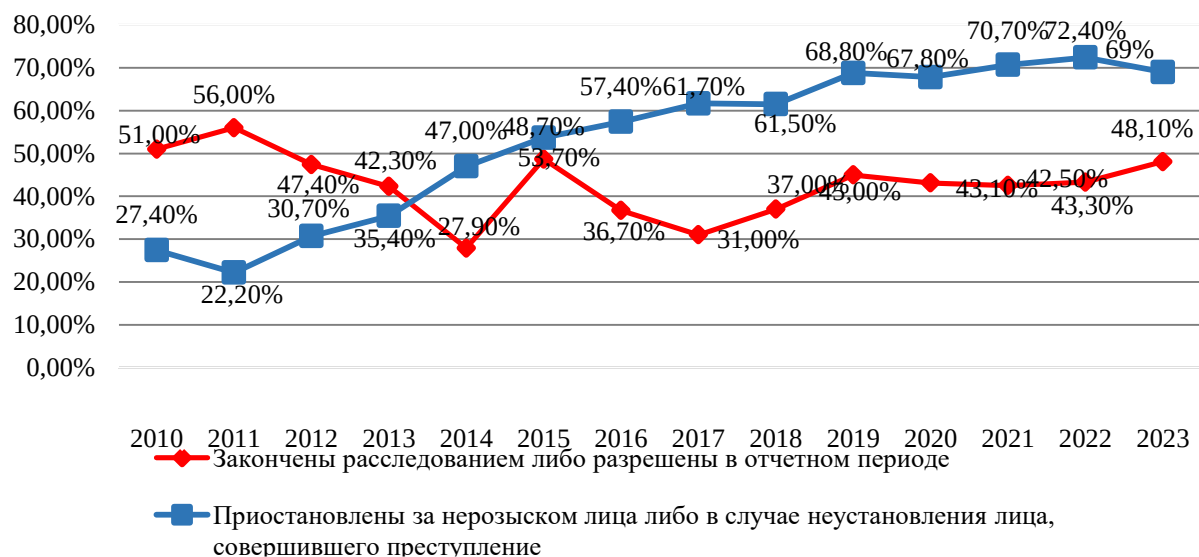


Диаграмма 11. Удельный вес уголовных дел в 2010-2023 гг., %

Таблица 11

Удельный вес уголовных дел, направленных в суд в 2010-2023 гг., %

Годы	Количество мошенничеств, уголовные дела о которых находились в производстве	Направлено в суд	
		Количество	Удельный вес
2010	1199	597	49,8%
2011	1819	998	54,9%
2012	2049	957	46,7%
2013	3148	1255	39,9%
2014	2805	665	23,7%
2015	2917	1302	44,6%
2016	3058	1045	34,2%
2017	3189	846	26,5%
2018	3274	1096	33,5%
2019	3356	1421	42,3%
2020	3920	1602	40,9%
2021	4095	1700	41,5%
2022	4207	1799	42,8%
2023	4295	1958	45,6%

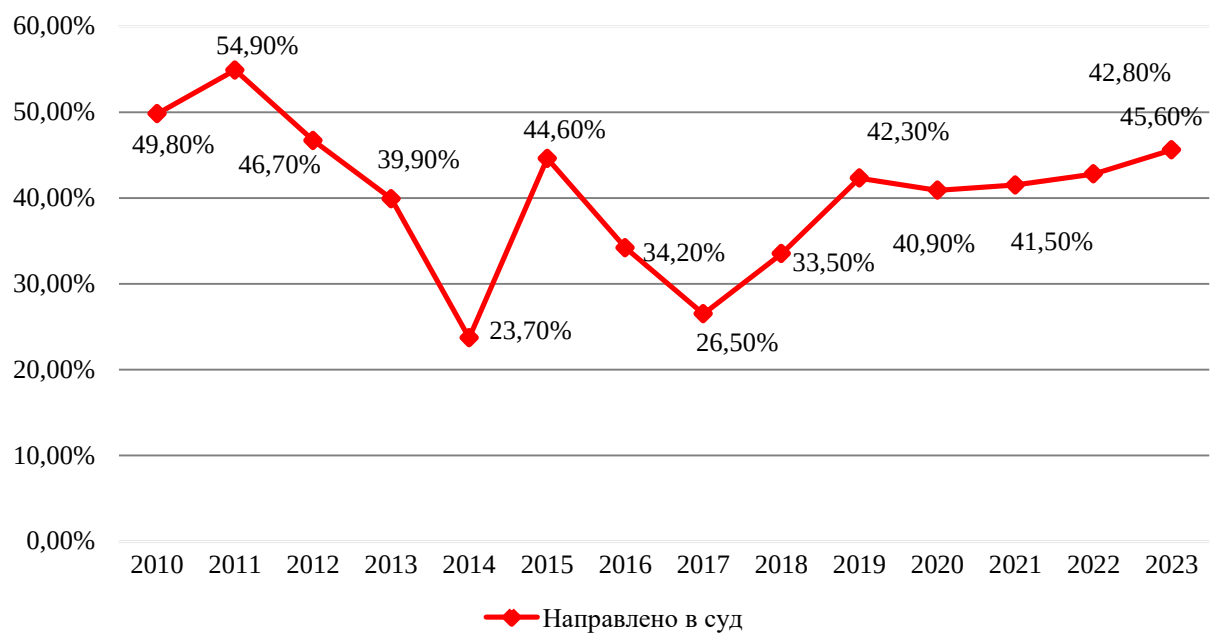


Диаграмма 12. Удельный вес уголовных дел, направленных в суд в 2010-2023 гг., %

Глава VI.

Противодействие перехвату оперативно значимой информации преступными элементами способом маскирования

В соответствии с действующими российскими стандартами перехват информации – это неправомерное получение данных с использованием технических средств, которое осуществляет поиск, прием и обработку информативных сигналов, т.е. сигналов, по параметрам которых можно восстановить защищаемую информацию. В свою очередь, не контролируемое носителем защищаемой информации распространение информации через физическую среду до технического устройства, которое осуществляет перехват информации, называется утечкой информации по техническому каналу.

В настоящее время организованные преступные группы включают в себя по иерархической лестнице лиц, имеющих специальное техническое образование и знания, которые они применяют при осуществлении различного рода преступных деяний. В ситуациях, когда сотрудники органов внутренних дел при проведении оперативно-розыскных мероприятий осуществляют документирование фактов, указывающих на преступную деятельность разрабатываемых лиц, преступники могут использовать полученные специальные знания для оказания различного рода противодействий, в том числе и перехвата информации.

6.1. Алгоритмы маскирующих преобразований видеоинформации

Возможность передачи видеоинформации является характерной чертой современных систем и сетей связи. Передача изображений в цифровой форме позволяет существенно повысить качество и объем видеоинформации, получаемой пользователями проводных и беспроводных сетей. Спектр приложений передачи видео чрезвычайно широк. Это не только ставшие востребованными в последнее время системы охранного телевидения, видеонаблюдения, дистанционного мониторинга, видеоконференций, но и многочисленные системы, обеспечивающие предоставление развлекательных сетевых сервисов.

Использование при передаче видеоинформации открытых сетей и сетей общего пользования ставит перед разработчиками систем передачи видео проблемы, связанные с опасностью использования этой информации несанкционированными пользователями. Конечно, проблема обеспечения целостности информации характерна не только для передачи видеоинформации

мации. Значительные усилия при создании открытых сетей тратятся на обеспечение безопасности информации. Однако для видео эта проблема имеет свои существенные особенности. Маскирование изображений (т.е. преобразование изображения к шумоподобному виду) требует учета специфики ее структуры, а также алгоритмов, используемых для сжатия и передачи видео.

6.2. Форматы данных. Избыточность и сжатие

Изображения и видео обладают большой избыточностью, поэтому для уменьшения объема передаваемой информации применяют сжатие. Большинство методов кодирования видео для достижения эффекта сжатия используют два типа избыточности: временную и пространственную. Во временной области имеется значительная корреляция между видеокадрами, зафиксированными в близкие моменты времени. Смежные по времени кадры имеют высокую степень корреляции, особенно при высокой частоте кадров. В пространственной области также наблюдается высокая зависимость значений пикселей, лежащих в кадре близко друг к другу. Следует отметить, что часто видеопоследовательности рассматривают как поток отдельных кадров и рассматривают эти кадры независимо.

Наибольшее распространение получили методы компрессии видео и изображений с потерей качества, которые основаны на психовизуальных особенностях зрительной системы человека и позволяют достичь высоких степеней сжатия. Сжатие изображения/видео выполняется кодером, восстановление изображения – декодером (часто кодер и декодер объединяют одним термином – кодек). В ходе разработки и реализации схемы маскирования видеoinформации рассматривались следующие форматы данных: BMP, JPEG, Motion-JPEG (M-JPEG), MPEG.

6.2.1. BMP

Формат BMP хранит непосредственно значения пикселей изображений и чаще всего не использует каких-либо схем сжатия (хотя в нем и предусмотрено сжатие без потерь) и не используется для передачи по сетям из-за большого размера файлов с изображениями. В данном проекте формат BMP используется только для демонстрационных целей.

6.2.2. JPEG

Формат JPEG был разработан для сжатия одиночных неподвижных изображений. Этот алгоритм позволяет осуществлять как очень высокие

степени сжатия, которым характерно низкое качество изображения, так и более низкие степени сжатия, обеспечивающие хорошее качество.

В схеме сжатия JPEG обработка изображения происходит следующим образом:

1) Цветовая модель RGB преобразуется в цветоразностную YUV. Изображение может содержать одну или несколько составляющих (components). Полутонное монохромное изображение содержит одну составляющую. Цветное изображение содержит несколько составляющих – яркостную Y и две цветоразностные Cr и Cb.

2) Для каждой компоненты (яркостная и две цветоразностные) выделяются подблоки пикселей размера 8x8 и выполняется дискретно-косинусное преобразование (DCT, discretecosinetransformation) каждого подблока. Данное преобразование концентрирует энергию сигнала в области нижних частот. Различают DC и AC коэффициенты. DC коэффициент характеризует среднее значение для подблока изображения.

3) Полученные значения квантуются согласно таблицам квантования. После квантования матрица приобретает треугольный вид, и большая ее часть равна нулю. Таблицы квантования определяют степень сжатия.

4) Полученная матрица с квантованными значениями преобразуется в вектор из 64 компонент при помощи зигзагообразного сканирования.

5) AC коэффициенты кодируются методом длин серий (RLE), DC коэффициенты соседних блоков коррелированы, поэтому подвергаются разностному кодированию.

6) Для дальнейшего сжатия полученные значения кодируются без потерь энтропийным кодером.

При кодировании DCT коэффициентов предлагается использовать код Хаффмана либо арифметический кодер. Но т.к. последний был запатентован и более сложен для реализации, он практически не используется в JPEG. Кроме того, в спецификации JPEG предусмотрено несколько режимов работы: последовательный (стандартный режим), прогрессивный, иерархический (позволяют отображать изображение с увеличением качества картинки), без потерь.

6.2.3. Motion JPEG

Формат Motion-JPEG был разработан для подвижных и видеоизображений. Фактически, формат M-JPEG рассматривает цифровой видеопоток как последовательность отдельных кадров, сжимаемых независимо друг от друга согласно схеме компрессии JPEG. Данный формат хорошо подходит для систем видеонаблюдения, так как в нем кадры обрабатываются по отдельности, что позволяет осуществлять быстрый по-

кадровый поиск, получать качественные стоп-кадры и отображать покадровое видео с регулируемой скоростью воспроизведения.

6.2.4. MPEG

Семейство стандартов MPEG было разработано специально для сжатия видеоинформации. MPEG, как и JPEG, представляет собой схему сжатия с потерями и основывается на аналогичных принципах - дискретно-косинусном преобразовании, квантовании и энтропийном кодировании.

Основной принцип MPEG сжатия - это сравнение двух последовательных образов, и передача по сети только небольшого количества кадров:

- опорных кадров (I-frames, intra-frames), которые содержат полную информацию об изображении и кодируются (сжимаются) независимо от остальных кадров;

- Р-кадров (predictiveframes), которые используют информацию из предыдущих кадров и отражают изменения относительно предыдущих кадров;

- В-кадров (bidirectionalframes), которые формируются на основе предыдущего и следующего кадра, что позволяет дополнительно повысить степень сжатия видео.

Кроме того, в форматах MPEG используется метод компенсации движения (motioncompensation), что позволяет дополнительно сжимать изображение.

MPEG обладает большей сложностью при кодировании и декодировании видеоданных, но позволяет достичь более высоких степеней сжатия, чем Motion-JPEG.

6.2.5. Особенности функционирования систем видеоконтроля

Для передачи телевизионного сигнала в системах видеоконтроля могут использоваться как защищенные цифровые линии связи, так и сети общего пользования (например, Internet), что накладывает дополнительные требования к конфиденциальности информации.

В настоящее время наиболее широко используются три типа систем передачи изображений по цифровым линиям:

- системы с компрессией изображений по принципу «условного обновления» (CR), предназначенные для передачи только информации об изменении изображения от кадра к кадру;

- системы с MPEG-компрессией, в которых используют специальные алгоритмы компрессии изображений движущихся объектов;

- системы с IPEO-компрессией, которые обеспечивают независимое сжатие кадра изображения.

Системы первого вида можно свести к частным случаям работы MPEG-сжатия. Изображения, передаваемые в таких системах, могут характеризоваться очень высокой степенью избыточности как временной (одна сцена на протяжении длительного времени), так и пространственной (например, абсолютно темное помещение). Все эти особенности должны быть учтены.

6.2.6. Особенности маскирования видеопотока и изображений

Схема маскирования/демаскирования должна работать независимо от кодера/декодера. Кроме того, при маскировании видеoinформации должно обеспечиваться следующее:

- недопущение уничтожения первичной информации, т.е. разрушение структуры сцены на изображении;
- недопущение уничтожения вторичной информации, т.е. сокрытие информации о характере передаваемого изображения (статичная/динамичная сцена, контрастная/темная сцена и т.п.). Данная информация может быть определена по размеру передаваемых кадров.

6.2.7. Соккрытие первичной информации

Под уничтожением первичной информации понимается разрушение структуры изображения, т.е. должно происходить полное уничтожение контуров объектов, должна отсутствовать возможность определения фона изображения, движения объектов на сцене (по последовательности кадров). Таким образом, в результате разрушения должно быть получено изображение, данные в котором по своим характеристикам близки к случайному шуму.

Часто в работах по защите видео подразумевается не полное маскирование информации, а лишь снижение качества до некоторого уровня, неприемлемого в коммерческом использовании видео (подразумеваются такие сервисы, как видео по требованию, онлайн вещание и т.п.). Пример такого типа маскирования приведен на рис. 16.

При защищенном кодировании также могут быть выбраны неподходящие режимы шифрования, в которых контуры сцены не разрушаются (примеры неудачного шифрования шифром ГОСТ в режиме простой замены для разных классов изображений приведены на рис. 17 и 18).

Кроме того, использование одинаковой ключевой информации при маскировании одинаковых изображений (либо областей изображения с одинаковыми оттенками) - особенно этому подвержен формат BMP - приводит к появлению одинаковых блоков в зашифрованном изображении, что раскрывает структуру изображения.

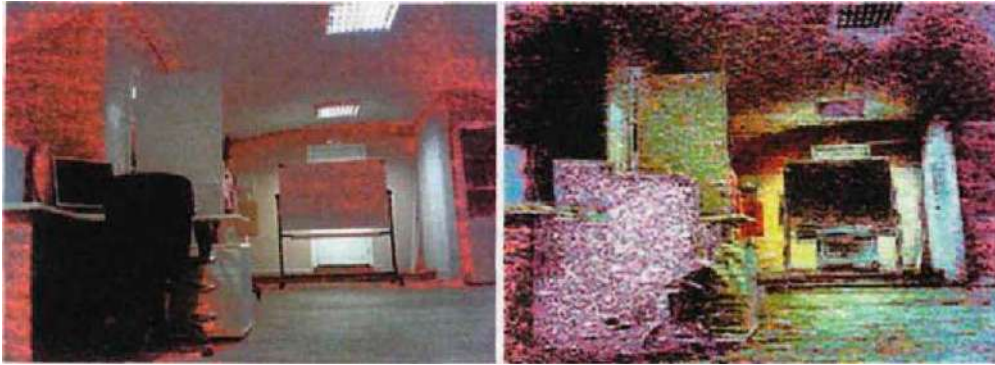


Рис. 16. Ухудшение качества изображения



Рис. 17. JPEG, ГОСТ простая замена

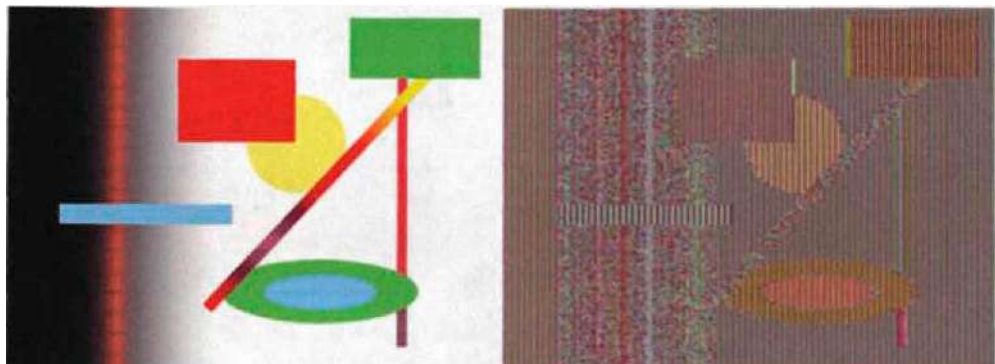


Рис. 18. BMP, ГОСТ простая замена

Пример полного разрушения структуры изображения при использовании алгоритмов шифрования в режимах с изменением ключа шифрования приведен на рис. 19.

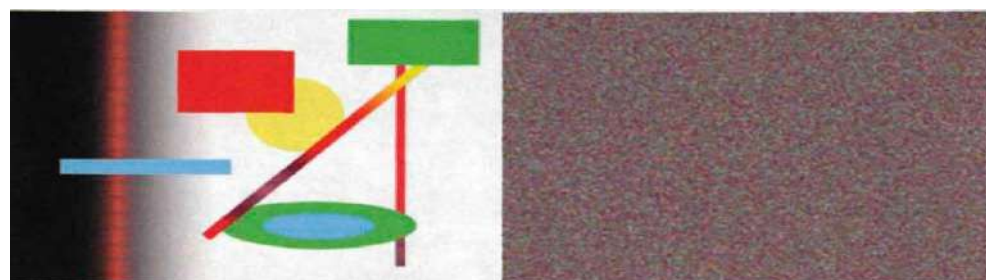


Рис. 19. BMP, ГОСТ гаммирование

Для шифрования JPEG файлов также необходимо применять режимы шифрования со сцеплением блоков, в противном случае структура изображения полностью не скрывается.

6.2.8. Соккрытие вторичной информации

Большинство применяемых на данный момент алгоритмов не имеют ограничения нижней границы кодирования. В частных случаях при использовании алгоритмов сжатия изображений/видео возможны ситуации, когда в зависимости от характера изображения (степени избыточности), происходит обработка последовательности кадров с различной степенью сжатия, что приводит к изменению объема передаваемой информации (битрейта). Например, если изображение обладает малой контрастностью, т.е. высокой пространственной избыточностью (например, темное помещение), передаваемые кадры будут сжиматься кодером с высоким коэффициентом, и объем передаваемой информации будет малым. И, наоборот, для сцены с насыщенной цветовой гаммой и большим количеством мелких объектов различной структуры, коэффициент сжатия окажется малым, и соответственно объем передаваемой информации будет большим. В кодерах, использующих для достижения эффекта сжатия временную избыточность, в случае длинной последовательности одинаковых кадров (например, неподвижная сцена) будет достигнута очень высокая степень сжатия. Таким образом, по объему передаваемых данных, в зависимости от кодека, можно сделать предположения о характере передаваемой картинки. В системах видеонаблюдения и удаленного мониторинга такая информация позволит сделать выводы о наличии/отсутствии движения в наблюдаемой области, о ее освещенности/контрастности, что крайне нежелательно.

Например, в последовательности кадров для сцены, на которой изначально изображено пустое помещение, после чего в помещении происходит некоторое движение - появляются новые объекты, возрастает размер передаваемых кадров на 15% (при фиксированном разрешении камеры и качества 1РЕО-сжатия).

Еще один пример приведен на рис. 20. В сцене б) появились новые объекты по сравнению со сценой а), что привело к увеличению размера сжатого кадра (с 2 кб до 7 кб) и отображению большей области для зашифрованного изображения.

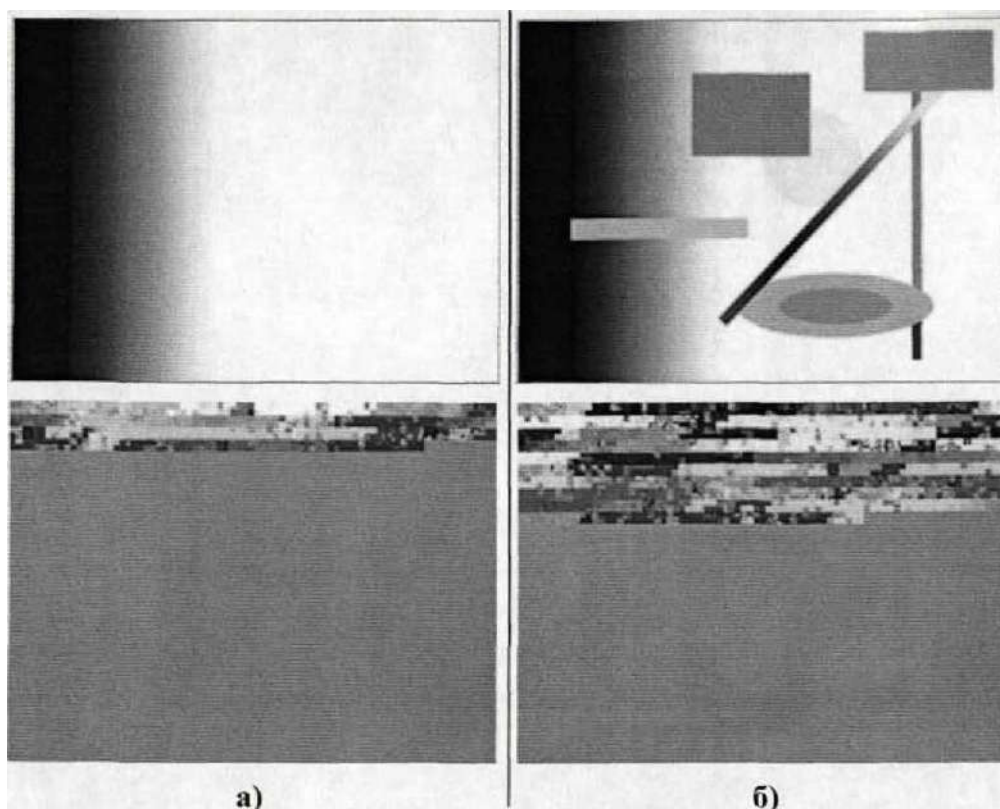


Рис. 20. Изменение размеров рисунков с появлением новых объектов

Поэтому, при создании систем с защищенной передачей видеоинформации, необходимо учитывать объем передаваемых данных за единицу времени. И при его снижении использовать методы, которые позволят защититься от распознавания характера передаваемого изображения по его объему. Например, можно дописывать к кадрам произвольные последовательности, которые в дальнейшем шифровать вместе с реальными данными и передавать в канал, что позволит избежать описанных выше ситуаций. Длину дописываемых последовательностей следует подбирать так, чтобы размер передаваемых кадров (опорных, вспомогательных) поддерживался на среднем уровне для заданного качества сжатия и разрешения видеокамеры.

6.3. Обзор существующих методов маскирования

6.3.1. Классификация методов

Условно все методы защиты видеоданных и изображений можно классифицировать тремя способами:

- 1) по типу обработки;
- 2) по уровню защищенности;
- 3) по совместимости со стандартными декодерами/устройствами воспроизведения.

По типу обработки можно выделить методы защиты данных, которые объединены с кодеком, и методы, которые работают независимо от кодека.

По уровню защищенности выделяют методы, которые полностью искажают исходные видеоданные, и методы, которые лишь снижают качество изображений и видео с целью невозможности их использования в коммерческих целях.

По совместимости со стандартными устройствами воспроизведения (проигрывателями), как программными, так и аппаратными, методы защиты медиа-данных можно разделить на 2 типа:

- полностью совместимые со стандартами и воспроизводимые без ошибок на стандартных проигрывателях;
- несовместимые, то есть те, которые вызывают ошибки на стандартных проигрывателях и не могут быть воспроизведены без специального декодера/проигрывателя.

6.3.1.1. Сплошное маскирование

Самый простой и надежный метод защиты – это «сплошное маскирование». В данном способе защиты весь сигнал изображения, получаемый от кодера или видео, рассматривается, как последовательность бит, и шифруется блоковым или потоковым шифром (например, алгоритмом шифрования ГОСТ 28147-89).

При этом необходимо отметить следующее:

- относительно высокие вычислительные издержки;
- несовместимость со стандартными проигрывателями;
- полное искажение исходных видеоданных, то есть высокая защита медиа-данных;
- маскирование/демаскирование выполняется отдельно от кодирования/декодирования;
- т.к. изображения и видео обладают особенностью - большая часть данных коррелирована или повторяется, необходимо использовать подходящий режим работы блокового шифра или стойкий потоковый шифр и использовать различные ключи для обработки различных кадров или блоков одного кадра;
- в зашифрованный таким образом видеопоток необходимо дополнительно вносить определенное число синхровставок, обеспечивающих синхронизацию шифратора и дешифратора.

При данном способе маскирования видеоданных стойкость определяется стойкостью используемого шифра.

На данный момент широко распространены методы шифрации видеоданных, обработанных кодером. Хотя, необходимо отметить, что суще-

ствуют и методы, использующие маскирование данных непосредственно перед их сжатием, после чего применяются алгоритмы сжатия без потерь. Такие методы являются развитием шифрования несжатых изображений и отличаются высокой ресурсоемкостью и снижением степени сжатия.

6.3.1.2. Методы с выборочным маскированием

С целью уменьшения вычислительной нагрузки при шифровании/дешифровании вместо сплошного шифрования предлагаются способы, обрабатывающие данные выборочно, т.е. маскирующие только ту информацию, которая наиболее критична для восстановления и отображения исходных видео и изображений. Выбор обрабатываемых таким образом данных производится на основе структуры графического формата. *В видео обычно используют маскирование следующих информационных компонент (или их комбинаций):*

- значения коэффициентов дискретно-косинусного преобразования (ЭСТ-коэффициенты), причем ОС и АС коэффициенты могут шифроваться различно (хотя маскирование только коэффициента ВС не дает эффекта, т.к. ОС отражает среднее значение и может быть определен по АС коэффициентам);
- знаковые разряды закодированных кодом Хаффмана БСТ-коэффициентов;
- опорные кадры (I-фреймы), интраблоки (I-blocks) в Р- и В-кадрах;
- вектор движения (значения, знаковые разряды).

Существует способ защиты видео, объединенный с процессом кодирования/декодирования. В процессе сжатия кадров для формирования вектора из 64 компонент используется зигзагообразное сканирование блока данных размером 8x8 пикселей. Вместо зигзагообразного сканирования авторы предлагают использовать произвольную перестановку. Данный способ вносит издержки – снижается степень сжатия и увеличивается битрейт. Кроме того, данный способ защиты видео подвержен атакам по известному открытому тексту и атакам только по шифртексту и не является безопасным, т.к. исходное изображение может быть восстановлено. Однако следует отметить, что такой метод может быть использован в случае, если отсутствует возможность атаки по известному открытому тексту, а также в случае, если значимость защищаемой информации невысока, т.е. атака на систему будет дороже, чем стоимость защищаемой информации.

Выборочное шифрование основывается на частотных распределениях пар байтов в видеопотоке MPEG. Утверждается, что байты кодированного видеопотока имеют равномерное распределение и внутри кадра (по крайней мере, в 1/16 части кадра) одинаковые значения байт практиче-

ски не встречаются. Согласно предложенному способу весь поток разделяется на 128-битные блоки, после чего каждый блок разбивается на две 64-битные последовательности согласно ключу. После этого обе последовательности объединяются друг с другом при помощи операции побитового сложения по модулю 2 (XOR) и одна из последовательностей шифруется одним из алгоритмов симметричного шифрования (рис. 21). Утверждается, что в случае, если поток не содержит повторяющихся блоков данных, четные байты представляют собой, так называемую, схему шифрования «одноразовый блокнот», который является абсолютно стойким, и безопасность всей схемы зависит от стойкости алгоритма шифрования, используемого в шифраторе.

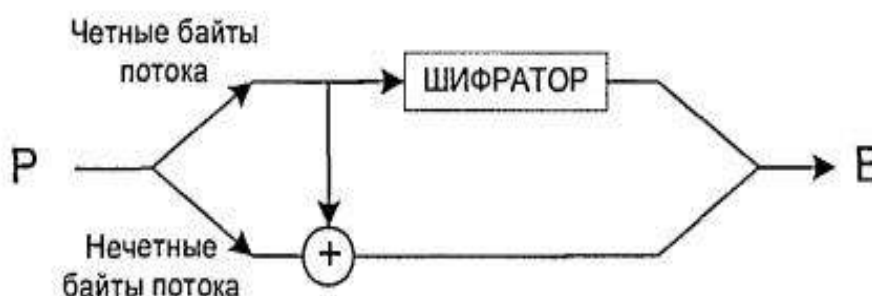


Рис. 21. Схема шифрования с распараллеливанием

Полученные значения представляют собой маскированную видеoinформацию и передаются получателю. Для затруднения криптоанализа предлагается схема выработки ключей, которая формирует переменные ключи для различных кадров, подблоков кадра и для разбиения последовательностей. Такой подход снижает вычислительную сложность примерно в 2 раза по сравнению со сплошным маскированием, но при этом теряется совместимость со стандартными кодеками. Кроме того, авторы утверждают, что схема устойчива как к атакам по известному открытому тексту, так и к атакам только по зашифрованному тексту (вероятность подбора нужных пар текста при статистическом анализе $\sim 2^4$).

Описанная выше схема опирается на равновероятное распределение значения байт в сжатых видеопоследовательностях. В действительности, при работе с различными типами изображений (деловая графика, фотореалистичные изображения, комбинированные) значения необязательно будут равномерно распределены (особенно это характерно для изображений деловой графики). В этом случае регулярные структуры (подблоки) последо-

вательности при использовании операции XOR для частей потока будут преобразовываться к регулярным структурам в зашифрованной последовательности. Таким образом, можно восстановить блоки изображения, и на кадре проявится некоторая структура сцены.

Есть способ для шифрования несжатых изображений (bmp формат). Предлагается разбивать изображения на битовые плоскости (например, для серого изображения 8 плоскостей) и шифровать (блоковым шифром) каждую плоскость отдельно. При этом старшие биты несут схожие черты относительно исходного изображения, а младшие – выглядят случайными. Авторы предлагают использовать данную особенность и шифруют младшие битовые плоскости. Такое маскирование добавляет шумы к исходному изображению. Но данный метод полностью не скрывает исходное изображение, а только снижает качество, при этом для значительного снижения качества необходимо шифровать 5 из 8 плоскостей.

Также возможно шифровать блоковым шифром AES битовые плоскости, соответствующие старшим разрядам пикселя. При этом показаны несколько атак на данную схему и утверждается, что для высокой защищенности необходимо шифровать как минимум 4 битовых плоскости. Такое маскирование также не приводит к полному маскированию исходного изображения, т.к. при визуальной оценке изображения просматриваются контуры и объекты сцены. Кроме того, данная схема неустойчива к атакам по известному исходному тексту.

Существует схема шифрования видеопотока MPEG, совместимая со стандартными проигрывателями и обеспечивающая выборочное маскирование. Кроме этого, в схеме используются параметры, определяемые пользователем, которые задают уровень маскирования видеоданных. Описанный алгоритм PVEA (PerceptualVideoEncryptionAlgorithm) оперирует с элементами видеопотока, закодированными кодовыми словами фиксированной длины (FLC, fixedlengthcodewords), к которым относятся:

- 1) intra-DC коэффициенты,
- 2) знаковые биты не intra-DC и AC коэффициентов,
- 3) знаковые биты и разностные значения векторов движения.

Для данных 3-х групп шифруемых элементов задаются вероятности, с которыми они шифруются. Данные вероятности позволяют задать степень маскирования данных. Само маскирование осуществляется симметричным шифром. Данная схема обеспечивает лишь частичное искажение качества, а не полное сокрытие исходных видеоданных, кроме того, некоторые виды атак также приводят к восстановлению исходной картинки до уровня, в котором отчетливо просматриваются объекты сцены.

Также существует еще один подход, отличный от описанных выше. Основная идея состоит в выборе такого способа сокрытия информации,

который будет устойчив к ошибкам передачи данных. Данная схема хорошо подходит для беспроводных каналов связи. Как известно, симметричные шифры основаны на идеях перемешивания и диффузии бит, и изменение в одном бите информации приводит к изменению всего блока данных. Поэтому при возникновении ошибок, которые не были исправлены на канальном уровне, дешифрация не даст исходное сообщение. В данной работе предлагается использовать такую функцию шифрования/дешифрования, которая не приводит к распространению ошибок. Показывается, что для построения этой функции нужно использовать операции перестановки и дополнения. Авторы также утверждают, что при выборе блока данных длины n , который будет преобразовываться, множество ключей (т.е. собственно множество функций) достаточно велико.

Данный подход может применяться как при выборочном, так и при сплошном шифровании, и может работать независимо от кодера/декодера.

Таким образом, можно отметить, что предлагаемые решения рассматривают сокрытие первичной информации с различной степенью защищенности – от полного искажения до частичной потери качества, но при этом не обращают внимания на уничтожение вторичной информации, т.е. на те признаки, которые дают злоумышленнику дополнительные сведения о сцене.

6.3.2. Алгоритмы симметричного шифрования

6.3.2.1. Алгоритм ГОСТ 28147-89

В России принят стандарт, обеспечивающий конфиденциальность данных – «Алгоритм криптографического преобразования данных ГОСТ 28147-89»³² является блочным алгоритмом с 256-битным ключом. Алгоритм базируется на архитектуре сети Файстеля, основным принципом которой является то, что процесс шифрования состоит из серии однотипных раундов. Основной шаг криптопреобразования, выполняемый в каждом раунде, включает три операции: 1) сложение с секретным ключом по модулю 2^{32} , 2) нелинейная подстановка на блоке замен и 3) циклический сдвиг влево на 11 разрядов. Блок узлов замен является секретным в алгоритме и не определен в стандарте, что позволяет увеличить стойкость алгоритма к различным типам атак.

³² С 1 апреля 2026 года ФНС России перешла на использование новых криптографических стандартов – ГОСТ 34.12-2018 и ГОСТ 34.13-2018, поддержка алгоритмов шифрования по ГОСТ 28147-89 прекращена.

ГОСТ 28147-89 предусматривает три режима шифрования данных:

- простая замена;
- гаммирование;
- гаммирование с обратной связью.

Также в стандарте определен дополнительный режим – режим выработки имитовставки, который служит для контроля целостности данных. Во всех этих режимах данные обрабатываются блоками по 64 бита, но в режимах гаммирования возможно обрабатывать неполный блок данных размером менее 64 бит. Режимы гаммирования представляют собой так называемые потоковые режимы работы блочного шифра.

В режиме простой замены исходные данные разбиваются на блоки по 64 бита, и каждый блок шифруется независимо от других блоков.

ГОСТ в режиме гаммирования позволяет шифровать данные в потоковом режиме. В этом режиме вырабатывается гамма (порциями по 64 бита), которая накладывается и снимается при помощи побитового сложения по модулю 2. Для генерации гаммы берется рекуррентный генератор последовательностей чисел (РГПЧ) с периодом T^n , выход которого шифруется в режиме простой замены, и полученное значение используется в качестве гаммы. Кроме того, для инициализации схемы (а именно, РГПЧ) должно быть задано начальное значение РГЧП – начальное заполнение, или синхропосылка, которую необходимо передавать принимающей стороне. Чтобы обеспечить уникальность гаммы шифрования, однозначно определяемой комбинацией «синхропосылка + ключ», необходимо использовать уникальную синхропосылку для каждого передаваемого сообщения. Так как ее секретность не требуется для обеспечения стойкости сообщения, синхропосылка обычно передается в открытом виде вместе с зашифрованным сообщением. Скорость данного режима определяется скоростью работы шифра в режиме простой замены.

Режим шифрования по ГОСТ гаммирование с обратной связью (или режим обратной связи по шифрованному тексту, СГВ) характеризуется тем, что в качестве начального вектора для формирования гаммы используется шифртекст, полученный на предыдущем этапе шифрования. Таким образом, происходит сцепление всех блоков данных.

6.3.2.2. Сравнение режимов шифрования

ГОСТ 28147-89 описывает маскирование как в режиме простой замены, так и в двух режимах гаммирования.

Режим простой замены имеет следующие особенности:

- независимое маскирование отдельных блоков и отсутствие распространения ошибок;

- проблема шифрования сообщений не кратных размеру блока: если последний блок данных не кратен 8 байтам, то необходимо его дополнять перед маскированием. При этом все полученные биты блока шифртекста будут значащими, необходимо хранить размер последнего блока, что приводит к увеличению размера шифртекста по сравнению с открытым текстом;

- одинаковые блоки зашифровываются в одинаковый шифртекст. При шифровании видеоданных такое недопустимо. Это главный недостаток данного режима.

Режим гаммирования:

- одинаковые блоки сообщения преобразуются в различные маскированные данные;

- возможность маскирования данных, не кратных 64 битам без дополнительных операций;

- при маскировании двух блоков данных в потоковом режиме недопустимо использовать один и тот же ключ и одинаковую синхропосылку, так как это ведет к потере стойкости системы обработки данных;

- изменения в некоторых битах маскированных данных после обратного преобразования приводят к изменению соответствующих битов исходных данных.

Режим гаммирования с обратной связью аналогичен режиму гаммирования, за исключением распространения ошибок:

- для начала обратного преобразования необходимо получить, как минимум, блок данных 64 бита;

- ошибка в одном бите маскированных данных распространяется на 2 блока данных: искажается 1 бит в соответствующем блоке исходных данных и полностью искажается следующий блок данных. Остальные биты маскированных данных обрабатываются без ошибок;

- т.к. каждый этап в режиме гаммирования с ОС зависит только от маскированного блока (который известен), возможно распараллеливание обратного преобразования.

Из выше сказанного следует, что для повышения стойкости защищенных видеоданных необходимо:

- использовать режимы маскирования, в которых одинаковые блоки видеоданных преобразуются в различные маскированные данные (гаммирование, гаммирование с ОС);

- использовать различные ключи при маскировании разных кадров;

- использовать различные синхропосылки при генерации гаммы.

6.3.2.3. Программная реализация ГОСТ

При оценке эффективности возможных программных реализаций главный интерес представляет реализация на 32-битовых платформах, так как 32-разрядные машины составляют в настоящее время большинство компьютерного парка.

При реализации на 32-битовых машинах наиболее трудоемкой операцией является замена. Предусмотренные ГОСТом подстановки в 4-битовых группах при программной реализации удобно попарно объединить и выполнять замену в 8-битовых группах, что существенно эффективнее. Надлежащая организация замены позволяет также избежать выполнения вращения слова на выходе функции шифрования, – если хранить узлы замены как массивы 4-байтовых слов, в которых уже выполнены необходимые сдвиги. Одна замена реализуется за три одноктактовые машинные команды: загрузка байта в индексный регистр, загрузка заменяющего значения в регистр, использование загруженного значения в операции побитового суммирования. В итоге перечисленные шаги оптимизации позволяют реализовать раунд шифрования по ГОСТ за 15 одноктактовых машинных команд. С учетом возможности процессоров IntelPentium по параллельному выполнению команд (технологии 88E2, 88E3), раунд ГОСТа может быть реализован за 8 тактов работы процессора, а весь процесс шифрования – за 256 тактов.

6.3.2.4. ГОСТ с редуцированным числом раундов

Для увеличения быстродействия алгоритма возможно использовать модификацию алгоритма ГОСТ с меньшим количеством основных шагов в базовых циклах. Этого можно достигнуть двумя путями – уменьшением длины ключа и уменьшением числа циклов использования элементов ключа. Число основных шагов в базовых циклах шифрования равно $N_{гп}$, где n – число 32-битных элементов в ключе, m – число циклов использования ключевых элементов; в стандарте $n = 8$, $m = 4$. Во сколько раз уменьшается число основных шагов в циклах, примерно во столько же раз увеличивается быстродействие кода.

Существует мнение, что в большинстве практических случаев представляется разумным использование редуцированных вариантов ГОСТа (также будем называть такой алгоритм «облегченный ГОСТ») без изменения схемы использования ключа $;/; = 4 = (3 + 1)$, но с уменьшенным вчетверо размером ключа ($n=2$) – это позволит увеличить скорость шифрования примерно вчетверо.

Необходимо отметить, что у редуцированного алгоритма снижается стойкость к различным методам криптоанализа. Хотя по стойкости к статистическим методам криптоанализа модификация ГОСТ с 64-битным ключом будет надежнее, чем DES с размером ключа в 56 бит, в работе приведен криптоанализ модифицированного алгоритма ГОСТ 28147-89:

- 20-раундового алгоритма GOST+, в раунде которого для наложения ключа используется операция XOR вместо сложения по модулю 2^{32} ;
- GOST-H, в котором, относительно оригинального алгоритма, изменен порядок использования подключей, а именно, в раундах с 25-го по 32-й подключи используются в прямом порядке, т.е. точно так же, как и в предыдущих раундах алгоритма.

6.4. Выбор маскирующего преобразования

6.4.1. Структура системы видеоконтроля с защищенной передачей

Общая схема работы системы защищенной передачи видео приведена на рис. 22. Предполагается отсутствие обратной связи с камерой. При этом рассматривается соединение камеры с сервером типа «точка-точка».

Маскирование и сжатие осуществляется различными устройствами, т.е. схема шифрования/дешифрования должна работать независимо от кодера/декодера. Для обеспечения полного маскирования видео используется сплошное маскирование потока закодированных видеоданных. В маскирующем устройстве используется алгоритм шифрования ГОСТ 28147-89 в потоковом режиме (режим гаммирования с обратной связью), что обеспечит наилучшую защиту данных с учетом их особенностей. При таком подходе шифратор работает отдельно от кодера и генерирует случайную последовательность, по которой невозможно восстановить исходное изображение, и стойкость зашифрованного потока определяется стойкостью алгоритма шифрования.

На этапе развертывания системы камере должен быть назначен уникальный идентификатор (ID) и выдан секретный ключ (МК, MasterKey).

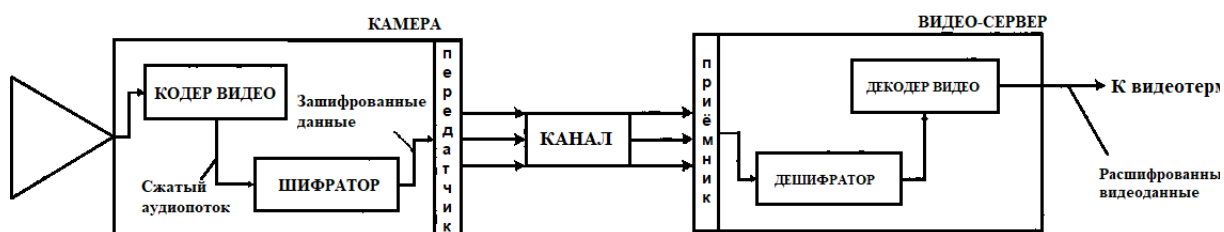


Рис. 22. Общая схема работы системы защищенной передачи видео

Идентификаторы и ключи хранятся также и на видеосервере и используются при обращении к камере. Предполагается, что к видеосерверу имеют доступ только легальные пользователи.

6.4.2. Схемы и режимы маскирования

Независимо от формата, в котором передаются данные, их можно рассматривать, как поток бит, и шифровать, используя различные схемы, которые имеют как свои достоинства – увеличение быстродействия, так и недостатки – снижение стойкости.

Приведенные ниже схемы могут применяться как в подходах со сплошным маскированием, так и с выборочным. При сплошном маскировании будут шифроваться все подряд данные, при выборочном – выбранные компоненты сначала должны группироваться в блоки и далее обрабатываться согласно схемам.

Под шифратором понимается алгоритм шифрования, работающий в одном из возможных режимов шифрования.

6.4.3. Маскирование потока бит видеоинформации

В данной схеме осуществляется маскирование потока бит (схема 6), где **P** – исходный открытый текст, **E** – шифрограмма. При этом шифрация может осуществляться либо блоковым алгоритмом в режиме сцепления блоков, либо алгоритмом шифрования, работающим в потоковом режиме.



Схема 6. Маскирование потока бит видеоинформации

Условно затраты на маскирование блока данных размером **L** бит можно оценить следующим образом:

- требуется один криптопроцессор, вырабатывающий гамму **L** бит (т.е. **A** операций);
- время шифрования – **t**.

Стойкость такой схемы определяется стойкостью алгоритма шифрования, но при этом имеется недостаток – временные затраты на маскирование. Эту схему можно ускорить, распараллелив потоки данных.

6.4.4. Маскирование половины потока бит видеоинформации

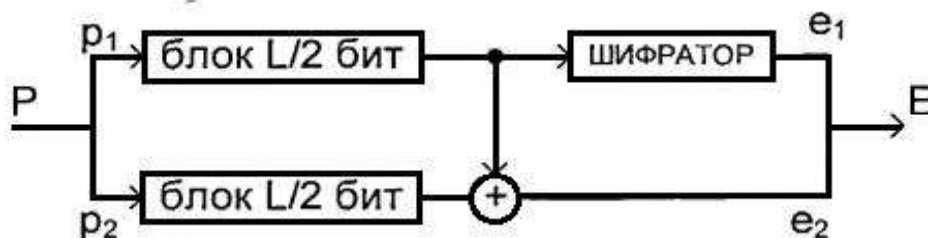


Схема 7. Маскирование половины потока бит видеоинформации

В данной схеме поток P разбивается на две части (либо согласно ключу, либо последовательно: нечетные биты – в верхний подблок, четные – в нижний), p_i -подблоки исходного текста, далее обе части складываются по модулю 2, и одна из них шифруется симметричным шифром. После этого части (e) объединяются, и зашифрованный поток передается в сеть. Для повышения секретности сбор зашифрованных битов может также выполняться согласно ключу.

Затраты в данной схеме следующие:

- один криптопроцессор, вырабатывающий гамму $L / 2$ бит (т.е. $A/2$ операций);
- 1 операция XOR;
- время шифрования – 112.

Данная схема за счет распараллеливания потока и шифрования по ГОСТ только одной половины более эффективна по времени и вычислительной сложности (надо выработать гамму $L/2$ бит).

Слабым местом схемы является наличие фактически незашифрованной последовательности, т.к. метод ее сокрытия (простой XOR) очень уязвим: в случае появления регулярных структур в блоке данных в зашифрованном сегменте также могут появиться регулярные структуры.

Таким образом, данная схема может быть использована только в предположении, что биты потока P равновероятны, и P не содержит повторяющихся сегментов. В случае, если P содержит одинаковые подблоки (в худшем случае $p_x = p_2$), зашифрованная последовательность будет неустойчива к статистическому анализу и можно сделать предположение о характере исходных данных.

Использование такой схемы в шифровании видео и изображений может привести к недопустимому падению стойкости из-за особенностей структуры графических форматов.

6.4.5. Параллельное маскирование разделенного потока бит видеoinформации

Чтобы избежать недостатков схемы 7, можно использовать маскирование обеих частей потока по схеме, приведенной ниже:

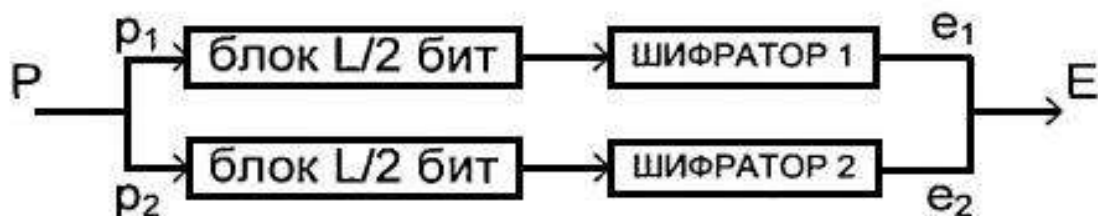


Схема 8. Параллельное маскирование разделенного потока бит видеoinформации

Затраты в такой схеме следующие:

- два криптопроцессора, оба вырабатывают гамму 2 бит (т.е. $2 - (A/2) = A$ операций);
- время шифрования – $1/2$.

В данной схеме требуется дополнительная информация для второго криптопроцессора, но при этом надежность схемы высока и не зависит от распределения бит в исходном потоке P. Кроме того, по вычислительной сложности данная схема аналогична схеме 6. Данная схема за счет распараллеливания потока и шифрования только одной половины более эффективна по времени и вычислительной сложности (надо выработать гамму $1/2$ бит).

Эта схема допускает развитие и дальнейшее ускорение за счет распараллеливания: добавляя криптопроцессоры, мы получаем пропорциональное уменьшение времени вычислений (но усложнение конструкции).

6.4.6. Использование схем облегченного маскирования

Для дальнейшего снижения вычислительной сложности можно использовать криптопроцессор, который в алгоритме шифрования использует меньшее количество раундов шифрования (например, в ГОСТ 16 раундов вместо 32). Таким образом, «облегченный» шифратор будет обрабатывать вдвое большее количество данных за то же время.

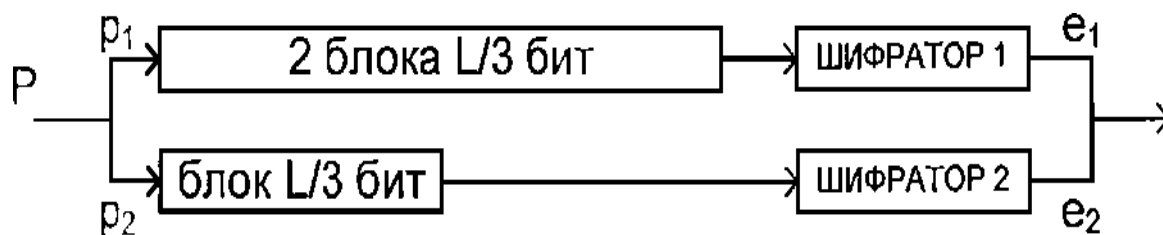


Схема 9. Облегченное маскирование

Затраты в такой схеме, представленной выше, будут следующие:

- требуется два криптопроцессора, при этом один использует 32 раунда, второй – 16 раундов шифрования. В сумме требуется $D / 3 + 2 - ((A / 2) / 3) = (2 / 3) D$ операций;
- время шифрования – $1/3$.

В данной схеме требуется более сложное разбиение потока. Это дает большее увеличение производительности.

6.4.7. Защита данных в формате BMP

В графическом формате BMP обычно отсутствует какое-либо сжатие (хотя и предусмотрен режим сжатия без потерь). Файл BMP содержит заголовков, описывающий параметры изображения (размер, разрешение, палитра, количество бит на пиксель и др.) и данные о цвете каждого пикселя изображения в модели RGB. Возможен вариант хранения данных, когда в заголовке файла описывается палитра (т.е. цвет) и для каждого пикселя указывается индекс в палитре.

В главе VI приведен обзор вариантов защиты информации при помощи шифрования различных комбинаций битовых плоскостей. Атаки и анализ таких способов показал, что в изображении может не полностью разрушаться структура сцены, и возможны атаки, восстанавливающие исходное изображение в довольно хорошем качестве. Поэтому для защиты полного сокрытия информации необходимо использовать сплошное маскирование либо блоковыми шифрами в режимах со сцеплением блоков, либо потоковыми шифрами. В этом случае стойкость будет определяться стойкостью шифра. Зашифрованные данные будут иметь случайный вид и будут отображаться как случайный шум.

6.4.8. Особенности кодирования Хаффмана в JPEG и маскирование

В зашифрованном изображении, сжатом по стандарту JPEG, при отображении проявляются однотонные полосы, которые периодически довольно резко меняют свой цвет. Кроме того, часто при заданном разрешении изображения отображается не вся область, а только некоторая часть (см. рис. 23).



Рис. 23. Зашифрованный кадр JPEG

Для объяснения таких эффектов в зашифрованных данных (т.е. фактически случайной информации) необходимо подробно описать формат сжатия JPEG, в частности, сжатие без потерь (энтропийное кодирование).

6.4.8.1. Структура данных, обрабатываемых кодером JPEG

Изначально, все изображение разбивается на блоки 8x8 пикселей. Такой блок называется единицей данных (DU, dataunit). Обработка ведется макроблоками, размер которых определяется в зависимости от типа изображения (цветное, оттенки серого). Согласно формату, такой макроблок называется минимальным кодируемым блоком (minimumcodedunit, MCU).

Для изображения в оттенках серого (grayscalemode) используется одна компонента – яркостная. В этом случае, MCU состоит из одного блока 8x8. Обход файла осуществляется построчно слева направо сверху вниз, и режим называется «без чередования» (non-interleavedorder).

Для цветного изображения обычно, а в основном режиме (baselinejpeg) – всегда используется три компоненты (одна яркостная (Y) и две цветоразностные (Cr, Cb). Так как глаз мало восприимчив к цветовой составляющей по сравнению с яркостной, для цветоразностных компонент обычно используется прореживание, что позволяет дополнительно сжать изображение.

Режим прореживания сохраняется в файле в поле маркера SOF и используется декодером при отображении изображения. Часто используется тип прореживания 4:2:0 (таким образом, из двенадцати блоков 8x8 пикселей получается шесть). В этом случае MCU состоит из шести блоков 8x8 (data units) (рис. 24). Обход компонент 60 определяется параметрами H1, и V1 для каждой компоненты в поле маркера SOF.

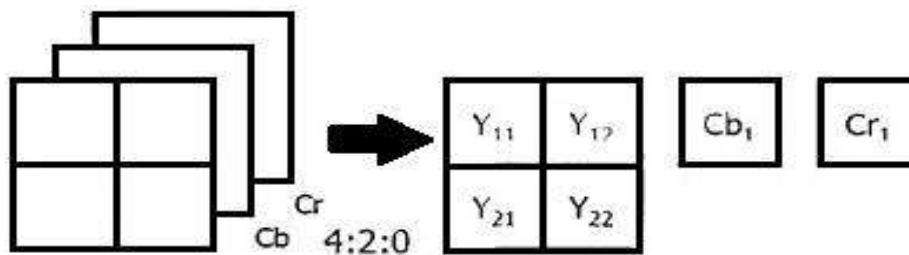


Рис. 24. Процесс прореживания в JPEG

Для приведенного на рис. 24 примера значения для яркостной компоненты: $H1 = 2$, $V1 = 2$, для Cr компоненты $H2 = 1$ и $V2 = 1$, для Cb компоненты $H3 = 1$ и $V3 = 1$, и MCU будет выглядеть так: Y_{11} , Y_{12} , Y_{21} , Y_{22} , Cb_1 .

Данные блоки 8×8 будут обработаны именно в такой последовательности (подвергнуты дискретно-косинусному преобразованию, проквантованы, сжаты без потерь) и сохранены в файл.

6.4.8.2. Энтропийное кодирование

Каждый MCU сжимается без потерь кодером Хаффмана (либо арифметическим кодером, который используется редко). Кодирование DC и AC коэффициентов осуществляется по-разному. Для кода Хаффмана используются таблицы кодовых слов, описание которых хранится в файле JPEG. Всего может использоваться до четырех таблиц:

- 1) таблица для кодирования DC коэффициентов яркостной компоненты;
- 2) таблица для кодирования AC коэффициентов яркостной компоненты;
- 3) таблица для кодирования DC коэффициентов цветоразностных компонент;
- 4) таблица для кодирования AC коэффициентов цветоразностных компонент.

6.4.8.3. Кодирование DC коэффициентов

Коэффициент DC соответствует среднему значению блока 8×8 и для соседних блоков DC принимает близкие значения. Поэтому DC-коэффициент сначала подвергается разностному кодированию, потом – кодированию Хаффмана. Сжатие DC включает следующие шаги:

- формируется значение $DIFF = C - D_0$, где C – значение DC i -го блока 8×8 , $D_0 = 0$ (дифференциальное кодирование);
- формируется пара (SIZE, AMPLITUDE), где AMPLITUDE – значение DIFF, SIZE – размер в битах, который требуется для хранения AMPLITUDE.

Следует отметить, что все возможные значения DIFF распределены по категориям. Номер категории совпадает со значением SIZE (например, SIZE = 0x3, номер категории: 3, всего значений $2^3=8$, возможные значения AMPLITUDE: - 7, ..., -4, 4, ..., 7 или в двоичном виде 000, 001...,111). Всего 16 категорий (таблица 12).

Таблица 12

**Распределение возможных значений DC коэффициентов
по категориям**

<i>Величины</i>	<i>Категория</i>	<i>Код для категории</i>	<i>Биты для величины</i>
0	0	00	—
-1,1	1	010	од
-3,-2,2,3	2	011	00,01,10,11
-7,-,-4,4,...,7	3	100	000,001,010,011,100, 101,110,111
-15,...,-8,8,...,15	4	101	0000,...,0111,1000,..., 1111
-31,...,-16,16,...,31	5	110	00000,...,01111,10000 ...,11111
-63,...,-32,32,...,63	6	1110	
-127,...,-64,64,...,127	7	11110	
-255,...,-128,128,...,255	8	111110	
-511,...,-256,256,...,511	9	1111110	
-1023,...,-512,512,...,1023	10	11111110	
-2047,...,- 1024,1024,...,2047	11	111111110	...
-4095,...,- 2048,2048,...,4095	12	1111111110	...
-8191,...,- 4096,4096,...,8191	13	11111111110	...
-16383,...,-8192, 8192,...,16383	14		...
-32767,...,-16384, 16384,...,32767	15		...

6.4.8.4. Кодирование AC коэффициентов

Для AC коэффициентов сначала применяется кодирование длин серий (runlengthencoding, RLE), потом – кодирование Хаффмана. *Общая схема, следующая:*

- для всего вектора из 63 AC коэффициентов формируются тройки (RUN, SIZE) AMPLITUDE, где RUN – число нулей перед текущим кодируемым AC коэффициентом, AMPLITUDE – значение AC коэффициента, SIZE – размер в битах, требуемый для хранения AMPLITUDE. Существуют ограничения: максимум нулей – 16, т.е. для RUN используется 4 бита (если перед ненулевым коэффициентом нулей больше 16, то используется пара (15, 0); если все оставшиеся коэффициенты в блоке 8x8 нулевые, то используется символ (0,0) – «EOB» (end-of-block)), максимальное значение SIZE – 16 (4 бита). Аналогично, как и для DC коэффициентов, все значения AMPLITUDE разбиты по категориям (см. таблицу 12);
- пары (RUN, SIZE) кодируются кодом Хаффмана согласно таблицам;
- закодированные AC коэффициенты имеют вид:
(код Хаффмана для пары (RUN, SIZE)) | (AMPLITUDE)

6.4.8.5. Однотонные полосы при маскировании

Как было сказано ранее, при отображении зашифрованного файла (в данном случае в поле с закодированными данными стоят случайные значения) проявляются однотонные полосы, которые периодически довольно резко меняют свой цвет (см. рис. 23). Это можно объяснить следующим образом.

ОС коэффициент для каждого блока отражает среднее значение, AC коэффициенты – уточняют значения пикселей в блоке 8x8. Код Хаффмана относится к неравномерным кодам, т.е. для более часто встречающихся значений используется более короткие кодовые слова. Анализ таблиц Хаффмана для БС коэффициентов яркостной и цветоразностных компонент (табл. 12 и 14) показывает, что наиболее вероятными (вероятность до 0,875) встречаются кодовые слова длины 2 и 3 бита. Согласно табл. 12 возможные значения, описываемые кодовыми словами такой длины, лежат в категориях 0-5 (значения от -31 до +31) для яркостной компоненты и 0-3 (значения от -7 до +7) для цветоразностных компонент. Т.к. БС перед кодированием Хаффмана подвергается разностному кодированию, такие небольшие значения разности (ОПТ) для БС соседних блоков влияют очень незначительно на изменения яркости и цветности блока, что не заметно глазу. Поэтому возникают однотонные полосы, которые иногда резко меняют цвет и яркость, если значение ОПТ попало в более высокую категорию (это происходит с вероятностью менее 0,125).

6.4.8.6. Неполное отображение кадра

Также часто при отображении зашифрованного файла выводится только часть кадра (например, отображается не 640x480, а только 640x320 пикселей).

Отображение не всего кадра происходит из-за того, что данные, которые были закодированы кодером Хаффмана, после шифрования имеют случайный характер (свойство шифрующих алгоритмов). При декодировании таких случайных данных неравномерному декодеру не хватает кодовых слов для полного заполнения всего кадра. Кроме того, периодически декодер не может найти в таблицах кодовое слово, что тоже приводит к ошибкам и пропускам бит.

6.4.9. Уничтожение первичной информации

6.4.9.1. Общие принципы сокрытия первичной информации в JPEG

Для обеспечения полного разрушения структуры изображения используется сплошное маскирование данных, т.е. шифруются сегменты ECS (данные, закодированные энтропийным кодером). Шифровать стандартные заголовки (сегменты маркеров), описанные выше, нет необходимости, т.к. часто они являются общедоступными. Более того, при шифрации этих общеизвестных полей, появятся лазейки для злоумышленника, который может попытаться осуществить атаки по известному открытому тексту.

6.4.9.2. Формирование и передача ключевой информации

Для повышения надежности шифрования предлагается использовать различные ключи при шифровании разных кадров видеопотока и шифровать кадры независимо друг от друга. Это позволит генерировать различные шифртексты для одинаковых кадров.

Для произвольного доступа и перехода по кадрам в защищенном видеопотоке необходимо снабдить дешифратор некоторой вспомогательной информацией, которая будет использована для синхронизации шифратора/дешифратора и выработки ключа для требуемого кадра. Также для функционирования алгоритма шифрования ГОСТ 28147-89 в режиме гаммирования с ОС необходимо задавать вектор инициализации.

Можно рассмотреть несколько способов формирования и передачи служебной информации:

1. Информация генерируется случайно в шифраторе и передается в открытом виде на дешифратор. Необходимо использовать надежный генератор случайных чисел, что в компактной камере затруднено.

2. Информация генерируется по некоторому правилу в шифраторе и передается на дешифратор. Генерирование информации по некоторому правилу позволяет привязать синхронизацию к некоторым параметрам системы (метка времени, счетчик кадров).

3. Информация генерируется по некоторому правилу в шифраторе и в дешифраторе и не передается. Очевиден недостаток: возможна рассинхронизация шифратора и дешифратора, и при отсутствии обратной связи с камерой восстановление начальной видеоинформации будет невозможно.

4. Информация генерируется по некоторому правилу как в шифраторе, так и в дешифраторе, и передается на дешифратор. Благодаря передаче служебной информации возможно восстановление и контроль синхронизации между шифратором и дешифратором.

Наиболее устойчивым является последний вариант, т.к. даже в случае рассинхронизации дешифратор может синхронизироваться с шифратором, используя передаваемую информацию. Таким образом, выбранная схема будет генерироваться и передаваться ключевая информация km_1 , различная для каждого кадра.

В качестве km_1 предлагается использовать 32-битный счетчик. Использование 32-битного счетчика позволит передавать непрерывно кадры с частотой 30 fps на протяжении 1657 дней, после чего ключи будут повторяться. Для повышения защищенности системы необходимо изменять секретный ключ камеры МК не реже 1 раза в течение данного периода. Кроме того, использование счетчика кадров позволит осуществлять произвольный доступ к зашифрованным кадрам.

Передавать km можно в заголовке кадра JPEG, используя пользовательские маркеры APPn. Вспомогательная информация будет передаваться в открытом виде, поэтому необходимо определить правила генерации ключевой информации, которые не позволят атакующему получить симметричный ключ шифрования.

Для обеспечения уникальности пары «ключ + синхропосылка» и возможности синхронизации в случае потерь кадров, синхропосылка должна генерироваться для каждого кадра независимо. Таким образом, синхропосылка в предлагаемой схеме создается в шифраторе и передается дешифратору в заголовке кадра.

6.4.9.3. Правила генерации ключей и синхропосылки

Для генерации ключей будем использовать хеш-функцию R, на вход которой подается идентификатор камеры ID , секретный ключ камеры МК и ключевая информация km_i .

В качестве функции хеширования R используется хэш-функция, определенная в российском стандарте ГОСТ Р 34.11-94³³, выходом которой является 256-битное значение, используемое как ключ шифрования кадра K .

Таким образом, симметричный ключ для каждого кадра генерируется следующим образом: $K_i = H(ID \parallel MK \parallel km_i)$. Для создания синхропосылки предлагается использовать 64 бита выхода хэш-функции, примененной к кадру (сегментам ECS), т.е. $IV = low_M\{H(ID \parallel MK \parallel frame)\}$.

В случае смены MK или начала нового цикла счетчика km_i необходимо перезапустить систему. Под перезапуском системы понимается задание нового секретного ключа камеры MK и обнуление счетчика km_i .

При использовании такого способа выработки ключей для шифрования кадров и режима шифрования гаммирования с ОС, безопасность схемы основана на стойкости алгоритма шифрования ГОСТ и секретном ключе камеры MK .

6.4.10. Уничтожение вторичной информации

Под вторичной понимается информация, по которой не прямо, а косвенно, можно охарактеризовать изображение. Применительно к цифровым данным такой информацией будет размер файла. Для защиты от раскрытия информации об изображении по размеру передаваемых данных предлагается перед маскированием дописывать к коротким кадрам случайную информацию, это позволит поддерживать размер передаваемых кадров на постоянном уровне. В то же время потребуется следить и за максимальным размером кадра и обрезать лишнее, как правило, эта обязанность возложена на кодер. Основная стратегия сокрытия – поддержание некоего постоянного эффективного размера кадра.

Добавление данных к кадрам хотя и увеличит издержки на передачу и загрузку канала, но не позволит злоумышленнику извлечь какие-либо данные о характере передаваемой картинки.

Определение эффективного размера кадра, до которого необходимо дополнять каждый кадр, описано ниже.

³³ ГОСТ Р 34.11-94 – государственный стандарт Российской Федерации «Информационная технология. Криптографическая защита информации. Функция хэширования» отменен приказом Росстандарта от 7 августа 2012 года № 216-ст. Вместо него введен ГОСТ Р 34.11-2012 – национальный стандарт Российской Федерации «Информационная технология. Криптографическая защита информации. Функция хэширования».

6.4.10.1. Вычисление эффективной длины кадра

В данном разделе вычисление эффективной длины было выполнено теоретически, согласно математической модели, после чего результаты были проверены экспериментально.

Построим вероятностную модель по таблицам Хаффмана, описывающим DC и AC коэффициенты. При разборе шума декодером важную роль играют области, описывающие размер поля данных каждого коэффициента.

Будем рассматривать данные, как некий неупорядоченный шум, распределенный по нормальному закону. Коэффициент DC соответствует среднему (яркостному или цветоразностному) значению блока 8x8, поэтому для соседних блоков он принимает близкие значения. Поэтому DC сначала подвергается разностному кодированию, потом – кодированию Хаффмана.

Коэффициент состоит из двух полей: SIZE и AMPLITUDE, где AMPLITUDE – значение разности с соседним блоком (DIFF), SIZE-размер в битах, который требуется для хранения AMPLITUDE.

При разборе шума мы имеем дело со случайными двоичными данными. Вероятность появления значения в некоем диапазоне будет равна $2^{-\text{SIZE}}$ в степени размера поля SIZE.

Для стандартной таблицы Хаффмана можно легко найти вероятности длин и диапазонов значений DC коэффициентов. Для более наглядного представления построим таблицу вероятностей для яркостных коэффициентов.

Таблица вероятностей яркостных DC коэффициентов по стандартной таблице Хаффмана приведена ниже:

Таблица 13

Вероятности значений яркостных DC коэффициентов

Категория	Длина кода	Кодовое слово	Вероятность	Значение	Общая длина
0	2	00	0,25	0	2
1	3	010	0,125	-1,1	4
2	3	011	0,125	-3,-2,2,3	5
3	3	100	0,125	-7,...,-4,4,...,7	6
4	3	101	0,125	-15,...,-8,8,...,15	7
5	3	110	0,125	-31,...,-16,16,...,31	8
6	4	1110	0,0625	-63,...,-32,32,...,63	10
7	5	11110	0,03125	-127,...,-64,64,...,127	12
8	6	111110	0,015625	-255,...,-128,128,...,255	14
9	7	1111110	0,0078125	-511,...,-256,256,...,511	16
10	8	11111110	0,00390625	-1023,...,- 512,512,...,1023	18
11	9	111111110	0,001953125	-2047,...,- 1024,1024,...,2047	20
		ошибка	0,001953125		

Под ошибкой понимаются все коды, отсутствующие в таблице Хаффмана. В зависимости от программной реализации декодера ошибка может не вызывать сбоя, например, в случае, когда последний коэффициент разбирается по ветке else алгоритма.

Из таблицы 13 видно, что если вероятность появления большего значения уменьшается, то вероятность появления длинных полей также уменьшается.

По таблице построим диаграмму вероятностей размера яркостного DC коэффициента (рис. 25).

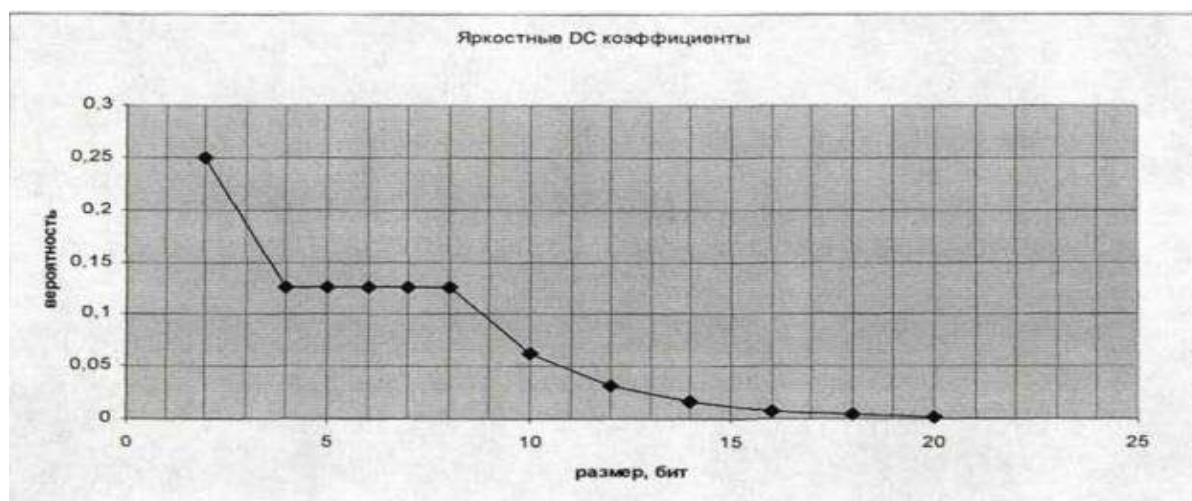


Рис. 25. Распределение вероятностей длины полей

Найдем среднее значение длины яркостных ОС коэффициентов, для них применима формула математического ожидания дискретной случайной величины (1):

$$M\xi = \sum_{i=1}^n p_i x_i \quad (1)$$

Подставив из таблицы вероятностей, в качестве p вероятности, а в качестве x длины коэффициентов, получим = 5,7 бит.

Таким образом, мы видим, что при интерпретации шума 1РЕО-декодер будет давать небольшие отклонения средней яркости блоков.

Найдем рассеивание длин ОС коэффициентов. Формула для дисперсии имеет вид (2):

$$D\xi = M(\xi - M\xi)^2 \quad (2)$$

Для дискретной случайной величины получим формулу (3):

$$D\xi = \sum_{i=1}^n (x_i - M\xi)^2 p_i \quad (3)$$

Суммируя все значения вероятности разности со средним размером, получаем дисперсию: $D_{\text{гхт}} = 14,5$.

Аналогичный расчет, используя соответствующие таблицы Хаффмана, можно провести и для АС коэффициентов. Всего в стандартной таблице Хаффмана для АС коэффициентов используется 161 кодовое слово (2). Проведем оценку их размера. Возьмем сводную таблицу 14 вероятностей размеров яркостных АС коэффициентов, построенную на основе стандартной таблицы.

Таблица 14

Вероятности появления яркостных АС коэффициентов

<i>Общий размер поля, бит</i>	<i>Сумма вероятностей полей</i>
3	0,25
4	0,3125
5	0,0625
6	0,15625
7	0,0625
8	0,078125
9	0,00390625
10	0,048828125
11	0,004394531
12	0,001464844
13	0,011230469
14	0,000488281
15	0,004150391
16	0,000732422
17	6Д0352Е-05
18	0,001083374
19	0,000183105
20	0,000198364
21	0,000213623
22	0,000228882
23	0,000228882
24	0,000228882
25	0,000244141
26	0,000244141
Ошибка	1,52588Е-05
<i>Общий размер поля, бит</i>	<i>Сумма вероятностей полей</i>

Диаграмма вероятностей появления яркостного АС коэффициента определенной длины приведена на рис. 26.

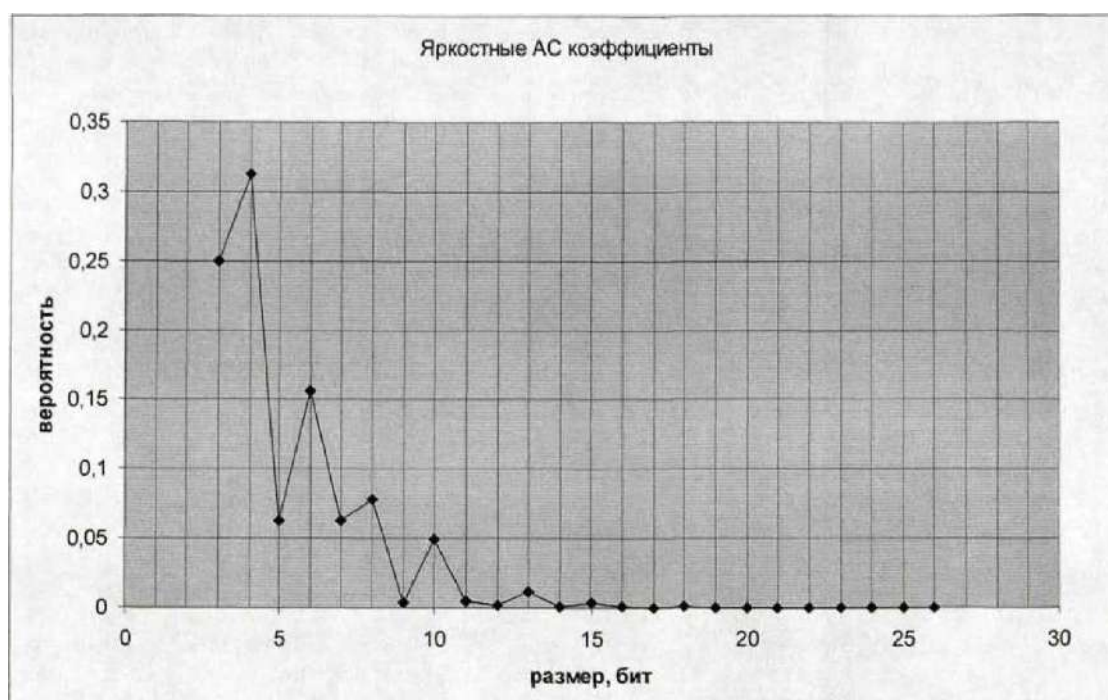


Рис. 26. Распределение вероятностей длины полей

На диаграмме видно, что распределение связано с неравномерностью используемого кода. По сводной таблице найдем математическое ожидание и дисперсию для одного такого коэффициента:

$$M_{DCY} = 5.19,$$

$$D_{DCY} = 5.92$$

Стандартом предусмотрена последовательность до 63 таких коэффициентов. Завершающим будет блок EOB (End-of-Block) длиной 4 бита и имеющий вероятность появления 0,0625.

Всего в последовательности может быть один коэффициент, с увеличением числа АС коэффициентов вероятность появления EOB будет изменяться следующим образом:

$$\begin{aligned} p_0 &= 0.0625 \\ p_1 &= p_0(1 - p_0) \\ p_2 &= p_0(1 - (p_1 + p_0)) \\ &\dots \end{aligned}$$

Таким образом, получаем общую формулу (4):

$$p_n = p_0 \left(1 - \sum_{i=0}^{n-1} p_i \right) \quad (4)$$

Приближенно будем считать случайные величины независимыми. Найдем среднее значение для 63 коэффициентов. Т.к. данная случайная величина дискретна, справедливы формулы, описанные выше: математическое ожидание количества АС коэффициентов будет равным $M_{\text{м}} = 13,73$.

Математическое ожидание блока яркостных АС коэффициентов будет равно сумме математических ожиданий его составляющих:

$$M_{\text{бАСУ}} = M_{\text{NY}} M_{\text{АСУ}} + EOB = 13,73 * 5,19 + 4 = 75,2$$

Аналогично, используя таблицы Хаффмана, можно оценить значения цветоразностных коэффициентов, для цветности синего и красного (Cr и Cb). Таблица вероятностей длин ОС коэффициентов приведена ниже.

Более наглядно данные этой таблицы можно представить в виде диаграммы, которая приведена на рис. 26. Здесь видно, что также, как и в случае с яркостными коэффициентами, большинство цветоразностных коэффициентов будут иметь небольшие размеры.

Математическое ожидание и дисперсия вычисляются по тем же формулам, что и для яркостных коэффициентов, и принимают следующие значения:

$$M_{\text{DCC}} = 4,24,$$

$$D_{\text{DCC}} = 6,95$$

По сравнению с яркостными ОС коэффициентами для описания цветоразностных коэффициентов требуется меньший объем данных.

Проведем расчет длин для соответствующих АС коэффициентов. По таблице Хаффмана построим сводную таблицу вероятностей их длин (табл. 15). Диаграмма вероятностей длин цветоразностных АС коэффициентов приведена на рис. 27.

Вероятности длин DC коэффициентов цветоразностных компонент

Категория	Длина кода	Кодовое слово	Вероятность	Значение	Общая длина
0	2	00	0,25	0	2
1	2	01	0,25	-1Д	3
2	2	10	0,25	-3,-2,2,3	4
3	3	110	0,125	-7,-,-4,4,...,7	6
4	4	1110	0,0625	-15,...,-8,8,...,15	8
5	5	11110	0,03125	-31,...,-16,16,...,31	10
6	6	111110	0,015625	-63,...,-32,32,...,63	12
7	7,	1111110	0,0078125	-127,...,-64,64,...,127	14
8	8	11111110	0,00390625	-255,...,128,128,..,255	16
9	9	111111110	0,001953125	-511,...,-256,256, 511	18
10	10	1111111110	0,000976563	-1023,...,-512,512,...,1023	20
11	11	11111111110	0,000488281	-2047,...,-1024,1024,.2047	22
		ошибка	0,000488281		

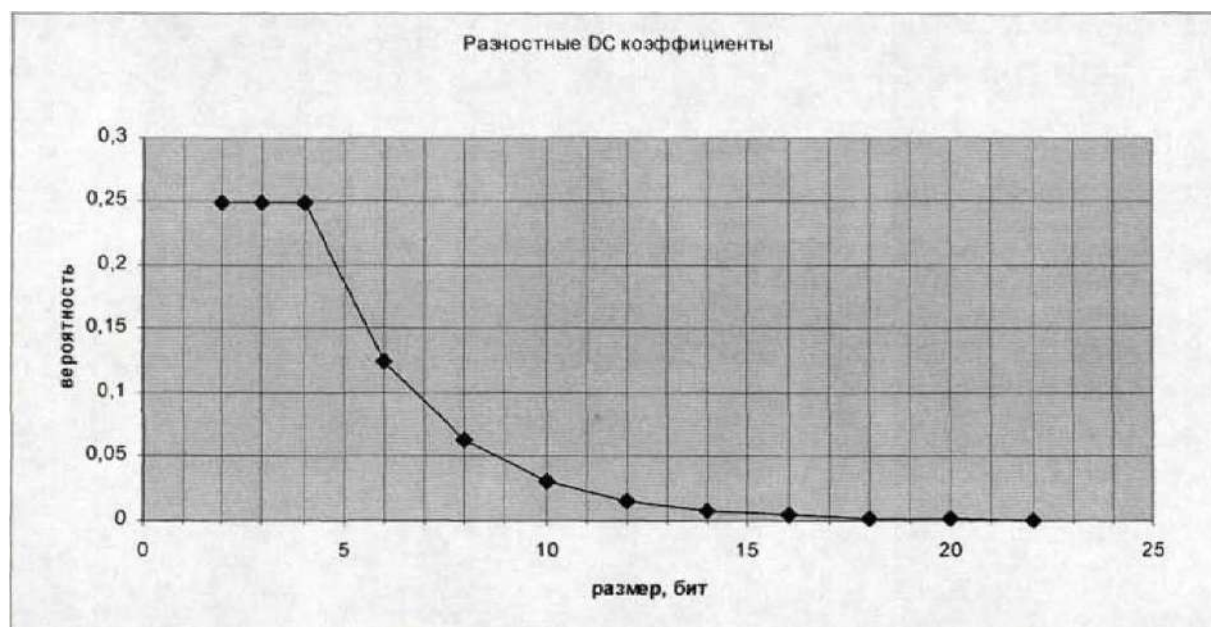


Рис. 27. Распределение вероятностей для яркостных DC коэффициентов

Так же, как и для яркостных АС коэффициентов, по стандарту возможна последовательность длиной до 63 коэффициентов. Завершающий блок EOB (End-of-Block) в данном случае будет меньше – всего 2 бита. Вероятность его появления будет очень высокой: 0,25.

Таблица 16

Вероятности АС коэффициентов

<i>Общий размер поля, бит</i>	<i>Сумма вероятностей полей</i>
2	0,25
3	0,25
5	0,1875
6	0,0625
7	0,09375
8	0,03125
9	0,03515625
10	0,047851563
11	0,005859375
12	0,017089844
13	0,004882813
14	0,0078125
15	6,10352E-05
16	0,00100708
17	0,001953125
18	0,000366211
19	0,001159668
20	0,000213623
21	0,000198364
22	0,000457764
23	0,000228882
24	0,000228882
25	0,000228882
26	0,000228882
Ошибка	1,52588E-05

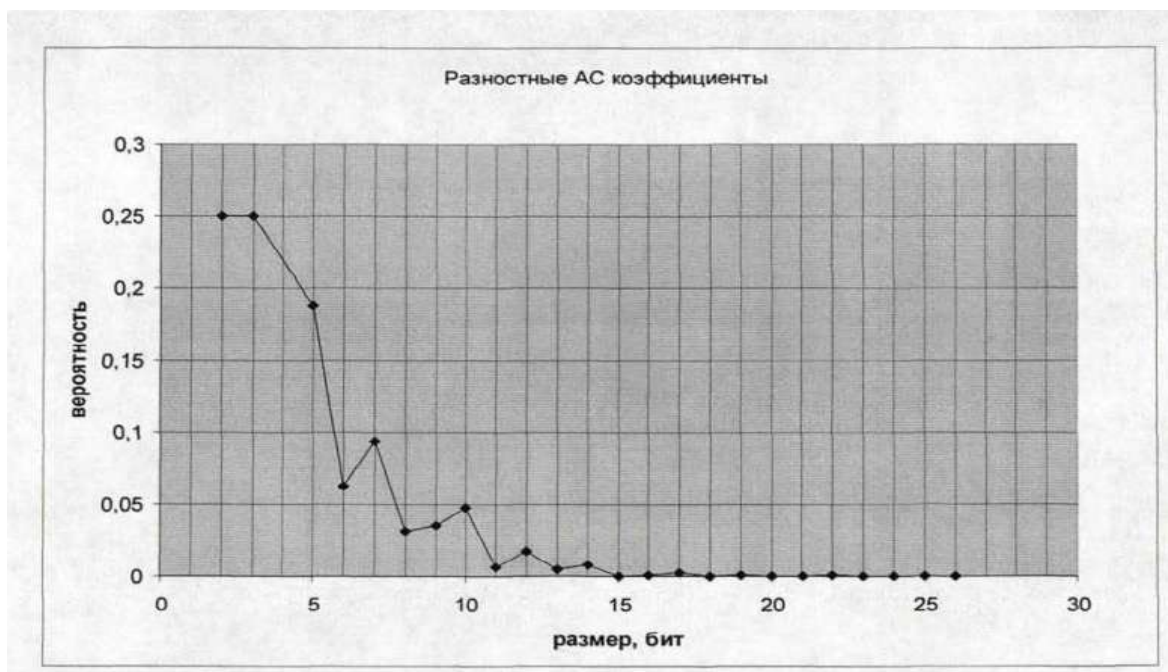


Рис. 28. Распределение вероятностей для цветоразностных АС коэффициентов

По формуле (1) для последовательности из 63 коэффициентов, с учетом их вероятностей, средняя последовательность будет представлена $MNC=3$ коэффициентами.

Математическое ожидание блока разностных АС коэффициентов будет равным:

$$M_{\text{бACC}} = M_{NC} M_{ACC} + EOB = 3 * 4.83 + 2 = 16.49$$

Рассчитаем полный размер отображаемого блока данных. Средний размер MCU будет равен сумме математических ожиданий составляющих его коэффициентов. Для изображения в оттенках серого 80 это будет один блок данных, представленный яркостными коэффициентами:

$$M_{MCU_{\text{серого}}} = M_{DCY} + M_{\text{бACY}} = 5.7 + 75.2 = 80.9 \text{ бит}$$

В таком режиме MCU будет кодировать блок из 64 пикселей, исходя из этого, можно определить «степень сжатия». Она будет равной 1,26 бит/пиксель.

Цветной MCU создается прореживанием блоков разных типов, и может кодировать области разных размеров. Для цветного изображения на размер блока будет влиять используемый метод прореживания компонент. Стандартом предусмотрено несколько типов чередования, наиболее распространенным является комбинация 4 яркостных и пары цветораз-

ностных компонентов. Это дает на блок 16 на 16 пикселей, его структура была представлена на рисунке 17. Далее для цветного изображения будем рассматривать только такую комбинацию коэффициентов.

$$M_{MCU_{цв}} = 4(M_{DCY} + M_{\delta ACY}) + (M_{DCCr} + M_{\delta ACCr}) + (M_{DCCb} + M_{\delta ACCb})$$

Так как таблицы Хаффмана для коэффициентов цветоразностных компонент (Cr, Cb) одинаковы, их можно считать равными. Таким образом, цветное изображение будет представлено четырьмя парами яркостных и разностных коэффициентов.

$$M_{MCU_{цв}} = 4(5.7 + 75.2) + 2(4.24 + 16.49) = 365.06 \text{ бит}$$

Исходя из того, что MCU кодирует блок из 256 пикселей, «степень сжатия» будет – 1,42 бит/пиксель. Из-за того, что JPEG-кодек является блоковым, критерий «степень сжатия» будет грубой мерой для расчета объема данных. Размер файла правильно соотносить с числом и структурой составляющих его блоков.

Оценим разброс значений размеров MCU. Найдем дисперсию для блоков изображения, рассмотрим ее как сумму дисперсий всех составляющих MCU:

$$D_{MCU} = D_{DC} + D_{\delta AC}$$

Количество AC коэффициентов в блоке точно неизвестно, поэтому за значение дисперсии блока возьмем сумму среднего числа коэффициентов:

$$D_{\delta AC} = \sum_{i=1}^N D_{ACi}$$

Коэффициенты между собой независимы, а дисперсии равны между собой, поэтому эту сумму можно заменить произведением и подставить в общую формулу:

$$D_{MCU} = D_{DC} + N * D_{AC}$$

Для цветного изображения в формулу добавятся цветоразностные компоненты:

$$D_{MCU_{цв}} = 4(D_{DCY} + N_Y * D_{ACY}) + 2(D_{DCC} + N_C * D_{ACC})$$

$$D_{MCU_{цв}} = 4 * (10.2 + 13.73 * 5.92) + 2 * (6.95 + 3 * 8.97) = 433.65$$

Определим разброс значений размера MCU, найдем среднеквадратичное отклонение для серого и цветного блоков:

$$\sigma = \sqrt{D},$$

$$\sigma_{\text{серого}} = \sqrt{91.48} = 9.56,$$

$$\sigma_{\text{цветного}} = \sqrt{433.65} = 20.82$$

Согласно теории вероятностей 99,73% всех значений будет попадать в диапазон трех среднеквадратичных отклонений в любую сторону от среднего. Оценим разброс объема данных, необходимых для отображения одного блока, в первом случае для серого MCU (8x8) это будет 80.9 ± 28.68 бит, а для цветного блока (16x16) получаем 365.06 ± 62.47 бит.

Таким образом, зная объем данных для одного блока MCU, можно найти эффективный размер кадра. Некоторые значения эффективных размеров кадров для различных типов изображений приведены в таблице 17.

Таблица 17

Значения эффективной длины для различных типов кадров (кбайт)

Разрешение	Оттенки серого	Цветной
160x120	2.96 ±0.09	3.34 ±0.76
320x240	11.85 ±0.35	13.34 ±3.04
640x480	47.4 ±1.40	53.46 ±12.20

Для оценки объема случайных данных для заполнения картинки без полос были проведены следующие эксперименты. Исследовались файлы изображений в формате JPEG с размером картинки кратной размеру MCU. Заголовки файлов содержали стандартные таблицы Хаффмана, блок данных после заголовка заменялся случайными данными. Заполнение производилось после блока Start-Of-Scan (SOS), обозначенного FFDA. Во избежание сбоя декодера на случайно появившемся маркере, в тексте блоки FF заменялись на FF00. В конце «шума» ставился маркер EOS. Таким образом, блок, заполненный случайными данными, находился между значениями блока FFDA до маркера FFD9.

Проводилась оценка изображения в несколько этапов:

- 1) Вычисление длины блока данных.
- 2) Подсчет числа блоков MCU (до начала фона, выдаваемого jpeg-декодером).

- 3) Расчет размера MCU при неполном заполнении картинки.

Для оценки размеров MCU изображения, представленного только одной яркостной компонентой, использовался тестовый файл `cameraman.bmp` (256 на 256 пикселей в оттенках серого), который был сохранен в jpeg с различным качеством, после чего блоки данных были заменены случайными значениями. Затем было проведено сопоставление отображенных блоков MCU с размером блока, данных заполненного шумом, результаты сопоставления сведены в таблицу 18.

Размер одного MCU для серого изображения составляет 8 на 8 пикселей. Исходное изображение и картинки, полученные путем отображения порций случайных данных, приведены на рис. 29. Параметр «качество» характеризует jpeg файл, согласно заголовку которого производится отображение картинки. Этот параметр определяется выбором таблицы квантования при сжатии.

Оценка цветного изображения была проведена путем сжатия тестового изображения `lena.bmp` размером 512 на 512 пикселей в jpeg с разным качеством. Блок данных после заголовка и до завершающего маркера так же, как и в случае с серым изображением, заполнялся шумом. Результаты оценки были сведены в таблицу 19.

Таблица 18

Экспериментальная оценка размера МСИ

<i>Качество</i>	<i>Блок данных, байт</i>	<i>Число МСИ</i>	<i>Размер МСЦ бит</i>
0	1392	123	90,53658537
10	2705	244	88,68852459
20	4252	409	83,16870416
30	5624	527	85,37381404
40	6704	685	78,29489051
50	7718	710	86,96338028
60	8833	843	83,82443654
70	10662	1011	84,36795252
80	13455	1024*	105,1171875
90	19922	1024*	155,640625
100	48961	1024*	382,5078125

Примечание: * означает полное заполнение изображения

Экспериментальная оценка размера цветного МСИ

Качество	Блок данных, байт	Число МСИ	Размер МСИ, бит
0	5136	105	391
10	8951	195	367
20	13368	292	366
30	17229	370	373
40	720866	443	377
50	24434	508	385
60	28486	604	377
70	34904	731	382
80	45960	991	371
90	74365	1024	581*
100	241769	1024	1889*

Примечание: * означает полное заполнение изображения

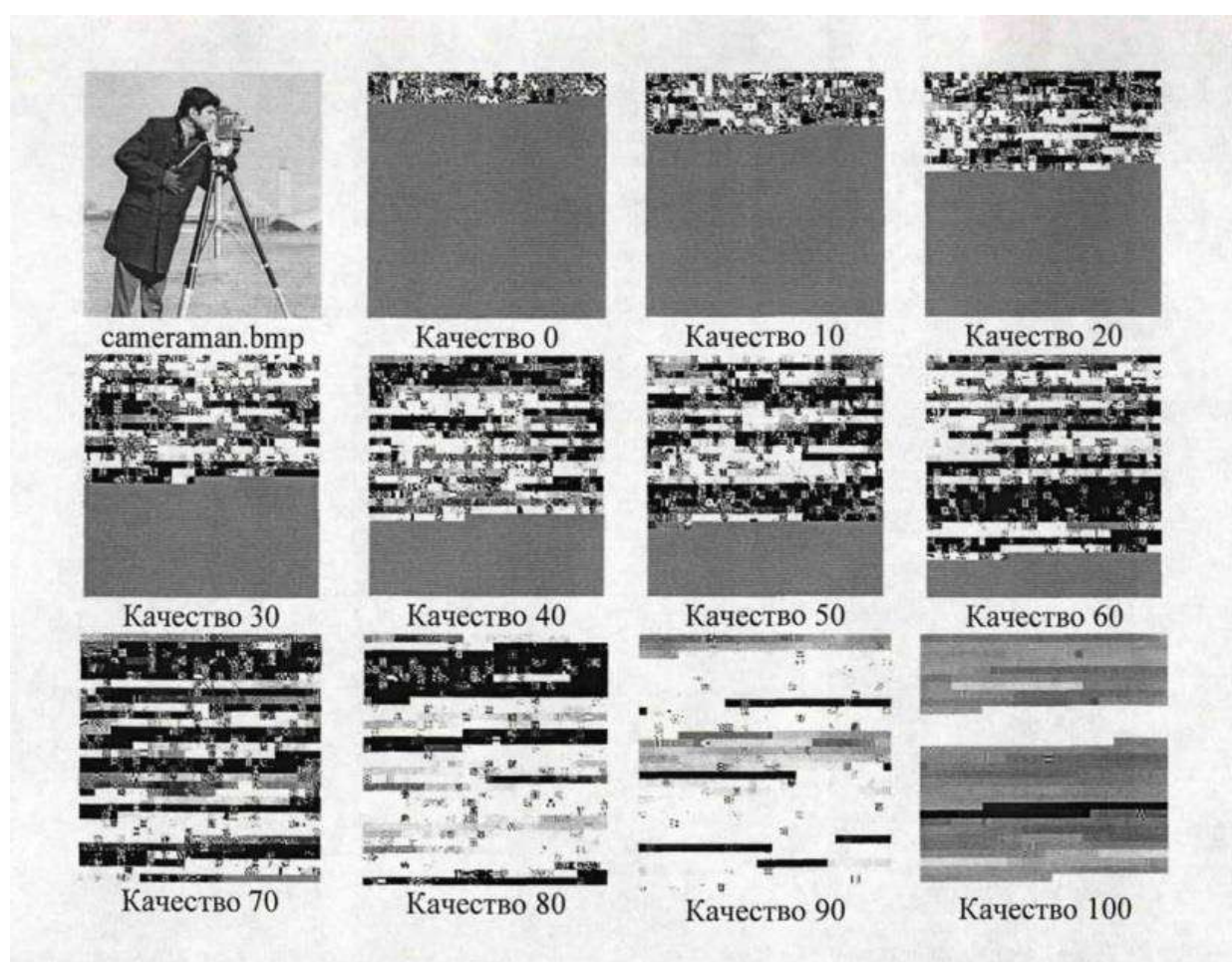


Рис. 29. Блоковый шум изображения в оттенках серого

Ошибки, приводящие к краху процесса декодирования, не проявились, на экране отображался шум. В ходе опытов проявилась блоковая структура шума в изображении.

Исходное изображение и изображения, полученные заполнением шумом, приведены на рис. 30. Размер МС и изображения каждого типа находится в пределах расчетной погрешности.

С увеличением качества характер картинок меняется – переходы между блоками становятся более плавными. Это связано с тем, что заголовки файлов для получения картинки требуемого качества, имеют разные таблицы квантования.



Рис. 30. Блоковый шум цветного изображения

Поскольку таблица квантования стандартом не регламентируется, она передается в заголовке выходных данных, т.к. знание таблицы квантования необходимо для последующего восстановления изображения.

Значения в таблице связаны с требуемым качеством картинки, т.к. таблица определяет минимальное значение, которое будет потеряно. При интерпретации эквивалентного объема шума, декодер, для изображений низкого качества, делает грубые переходы между блоками, в высоком

качестве переходы между значениями минимальны – это приводит к появлению больших однотонных полос. Рассмотренный в эксперименте подход применим и к оценке зашифрованных файлов изображений.

6.4.11. Возможные методы анализа вторичной информации

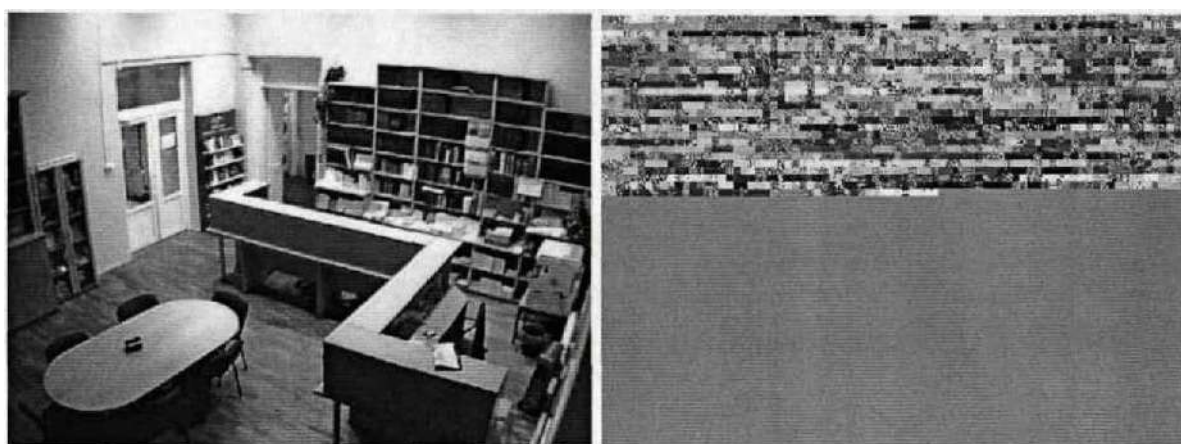
Рассмотрим возможные методы анализа вторичной информации, остающейся после выполнения процедуры маскирования изображения, используя для этого классические уровни атак.

6.4.11.1. Анализ без использования какой-либо дополнительной информации

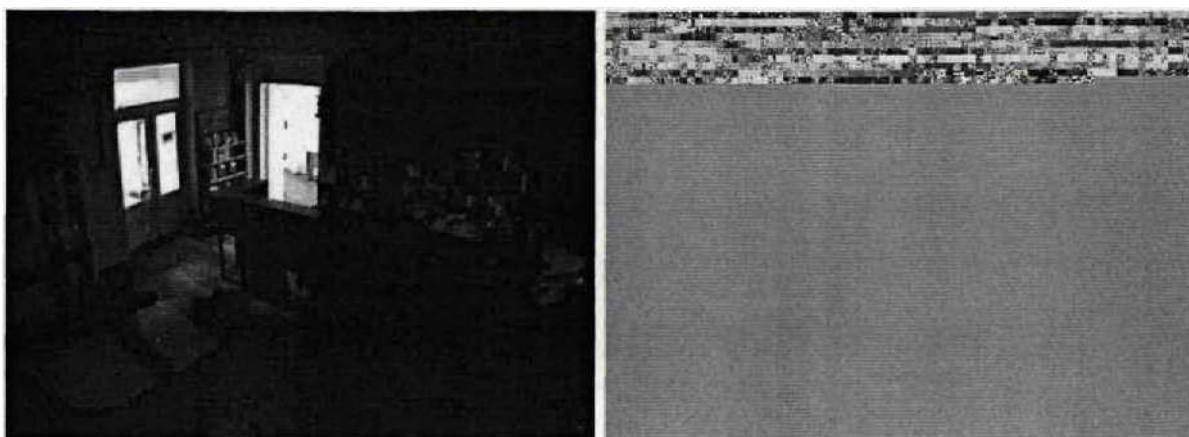
В этом случае, используя доступную преобразованную в результате процедуры маскирования видеоинформацию, можно оценить насыщенность передаваемого изображения или наоборот однотонность изображения и отсутствие большого числа различных фрагментов.

Например, легко определить, имеем ли мы дело с видеофрагментом, представляющим хорошо освещенную сцену со множеством деталей, или это подвергнутый обработке маскирования однотонный темный кадр. В первом случае размер маскированного кадра будет практически совпадать со стандартным размером видеоизображения, а во втором случае маскированный кадр будет существенно меньшего размера.

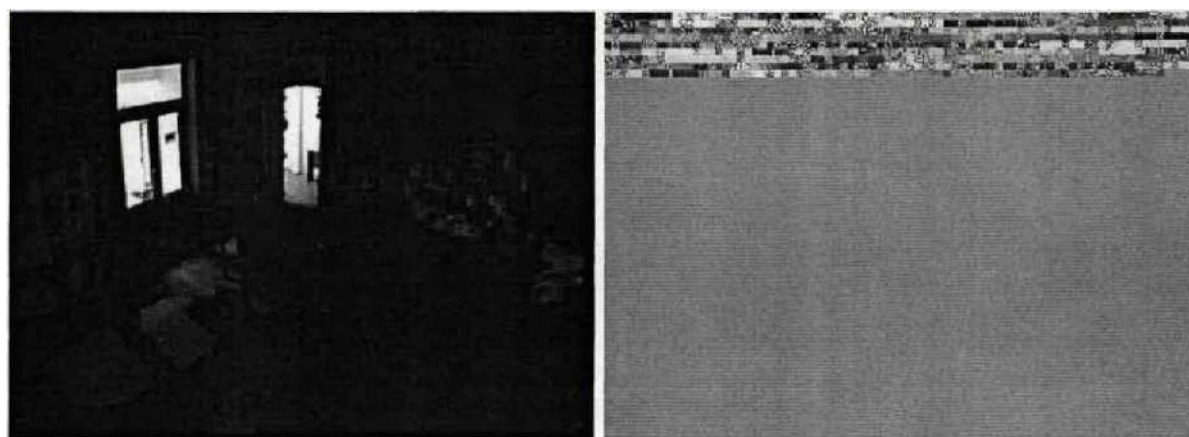
Например, возьмем стадии завершения рабочего дня в помещении, снятые IP-камерой видеонаблюдения (Genius IPCam Secure- 300R). Исходные и маскированные видеокadres, полученные при различном освещении сцены, представлены на рис. 31 (а - б).



а) Ярко освещенное помещение



б) В основном помещении погашен свет



в) Освещение отключено

Рис. 31. Исходные и маскированные видеокадры

Настройки камеры во время работы были неизменными: разрешение 640 на 480 точек, максимальная степень сжатия. Размер типичных кадров сведен в таблицу 20.

Таблица 20

Размеры видеокадров в зависимости от освещения сцены

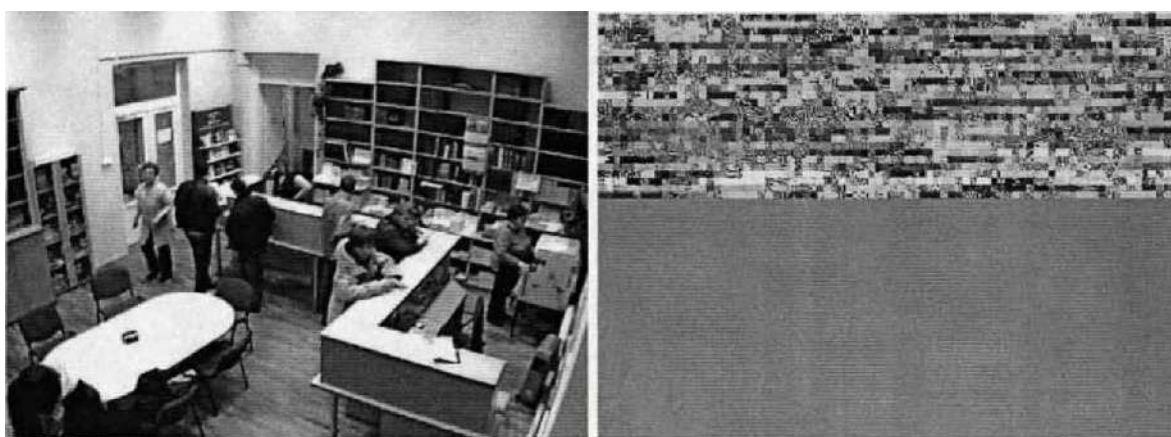
<i>Изображение</i>	<i>Размер байт</i>
а) Ярко освещенное помещение	26 150
б) В основном помещении погашен свет	11 208
в) Приглушен свет в дальнем помещении	9 868
г) В дальнем помещении свет погашен	8 990
в) Освещение отключено	6 950

6.4.11.2. Анализ при использовании пар исходного и маскированного изображения

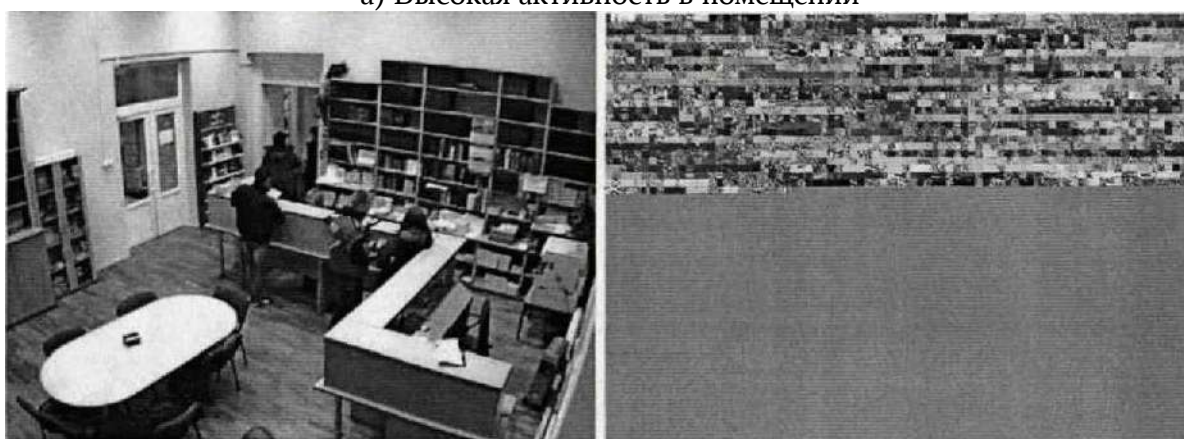
При возможности получения доступа к большому числу разнообразных обработанных и исходных видеофрагментов можно более точно провести классификацию маскированных изображений по их размеру, соотнеся размер анализируемого кадра формата jpeg и возможное исходное изображение.

Так, например, имея набор кадров одного и того же места в различных ситуациях (наличие машин, людей или их полное отсутствие), можно с высокой степенью достоверности соотнести размер доступного маскированного кадра с ситуацией на месте, изображение которого передается. Пример такой зависимости приведен на рис. 32 (а - б).

Размер файла кадра в первом случае составил 28 011 байт, а во втором – 26 495 байт, по сравнению с размером изображения пустого помещения разница в размере составляет 7,1 и 1,3 % соответственно.



а) Высокая активность в помещении



б) Низкая активность

Рис. 32. Зависимость объема маскированного кадра от активности в сцене

6.4.11.3. Анализ по выбранному исходному изображению

Эффективность и оперативность анализа вторичной информации существенно повышаются, если интересуется только наличие или отсутствие конкретной ситуации на месте, маскированное изображение которого удалось получить.

Следует так же отметить, что при анализе вторичной информации могут использоваться два подхода. Так как зашифрованные, т.е. фактически случайные данные, стандартным декодером декодируются и отображаются без ошибок, возможен визуальный анализ по не прорисованной части изображения. Второй подход – детальный разбор каждого блока МСи, входящего в кадр, без использования визуального сравнения и анализ бит, требуемых для заполнения кадра.

■ Выбор метода сокрытия вторичной информации

При дополнении кадра до эффективного размера можно использовать следующие данные:

1) Случайные значения, и не шифровать их. Подразумевается, что в системе присутствует генератор шумов. В качестве таких «абсолютно» случайных значений, например, могут использоваться значения токов утечки на диодах в микросхемах камеры. Такой способ генерации случайных значений требует наличия дополнительных микросхем и предъявляет дополнительные технические требования к камерам видеонаблюдения.

2) Зашифрованный соответствующее количество раз последний блок данных или некоторый шаблон, зашифрованный выбранным алгоритмом шифрования (с полным или сокращенным числом раундов). Как известно, статистические характеристики значений на выходе шифраторов близки к равновероятным случайным значениям, поэтому, можно использовать выход шифратора для генерации шума.

Данный способ предлагается использовать в схеме защиты видео.

Кроме того, добавлять данные можно либо для каждого MCU, либо для всего кадра. Добавление случайных данных после каждого MCU, размер которого меньше $M_{мси}$, неэффективно, так как требуется анализировать поток данных, разбивать его на макроблоки MCU и только после этого дописывать значения, при этом запоминая длину дописанных данных. При дешифрации этот вариант также значительно усложнит схему.

Вариант с дополнением до эффективного размера после всех блоков MCU более эффективен. Кроме того, запоминать длину дописанных (либо значащих данных) нет необходимости: зная структуру JPEG кадра, можно воспользоваться маркером конца кадра как признаком окончания значащих данных. То есть будем шифровать все значащие биты всех MCU и биты маркера EOI, после чего будем дописывать случайные значения нужной

длины, после которых поместим новый (незашифрованный) маркер EOI. При дешифрации первый встретившийся маркер EOI будет служить признаком того, что значащие биты закончились, а оставшиеся биты до следующего кадра (т.е. до маркера SOI) можно отбросить.

Таким образом, каждый кадр должен дописываться/обрезаться до размеров, приведенных в таблице 17.

Также возможны два подхода, реализующие дополнение до эффективной длины: использование фиксированной эффективной длины на протяжении всей работы камеры и адаптивное вычисление эффективной длины.

■ *Фиксированная эффективная длина кадра*

В данной схеме предполагается вычисление эффективной длины для заданных таблиц Хаффмана и ее использование на протяжении всей работы камеры. Как правило, размер кадра лежит в определенных пределах и имеет верхнюю и нижнюю границы. Для исключения возможности анализа вторичной информации требуется получить единый размер для всех кадров, получаемых с камеры. Верхнее ограничение возложено на кодер, если такого ограничения нет – файл кадра будет обрезаться алгоритмом защиты. А нижнее – на наш алгоритм защиты данных, который будет дописывать к зашифрованным данным некоторые случайные значения.

■ *Адаптивные методики для расчета эффективной длины*

Адаптивные методики базируются на анализе потока данных, генерируемых камерой за определенный промежуток времени. Цель анализа – найти эффективный размер кадра. Эффективным размером будет считаться максимальный размер кадра за этот период, это размер задаст нижнюю границу размера кадров. Основным недостатком адаптивной методики является невозможность учета нештатных ситуаций, вызывающих большой скачек передаваемых данных. Поэтому для такой методики необходимо задавать пределы, в которых будет находиться размер: при недостатке – добавлять данные, при избытке – обрезать.

Возможна реализация с однократной адаптацией на этапе инициализации системы и с непрерывной адаптаций, что позволит более эффективно использовать пропускную способность канала.

Глава VII.

Маскирование, основанное на методах теории помехоустойчивого кодирования

В предыдущей главе работы анализировалась эффективность использования алгоритмов блочного шифрования с изменяющимся ключом для обработки видеоинформации. Существенной проблемой такого подхода является необходимость обеспечения синхронного использования ключевой последовательности на приемной и передающей стороне и соответственно необходимость синхровставок в передаваемую информацию. Кроме того, в таких системах и передающая, и приемная сторона обладают всей необходимой информацией (ключ, алгоритм, устройство) для шифрации и дешифрации передаваемых и обрабатываемых сообщений. Таким образом, компрометация передающего устройства приведет к раскрытию всей конфиденциальной информации.

В ряде ситуаций передающее устройство, в отличие от приемного, находится вне контролируемой зоны и соответственно может быть доступно несанкционированному пользователю. При такой постановке задачи особенно важным видится разработка системы обработки (шифрации) видеоинформации, имеющей несимметричную схему, то есть системы, в которой получение доступа к устройству обработки информации на передающей стороне не приводит к полной компрометации всей системы. В настоящей главе для решения этой задачи используются коды, исправляющие ошибки.

7.1. Система МакЭлиса несимметричного шифрования, использующая коды, исправляющие ошибки

Хорошо известно, что задача декодирования помехоустойчивого кода с исправлением случайных ошибок в пределах корректирующей способности кода, в общем случае, является ТГР- сложной задачей. Сложность декодирования может быть существенно снижена (до полиномиальной) при наличии у кода конструктивного алгоритма декодирования. Одним из классов кодов, имеющим такой конструктивный алгоритм декодирования, являются коды, предложенные В.Д. Гоппой в 1970 году. Коды Гоппы задаются двумя объектами — множеством локаторов (нумераторов) позиций - $\mathcal{B}$ и многочленом Гоппы $g(x)$.

q -ичный вектор длины n $a = (a_1, a_2, \dots, a_n)$ является кодовым словом (L, g) - кода Гоппы, если выполняется следующее сравнение:

$$\sum_{i=1}^n a_i \frac{1}{x - \alpha_i} \equiv 0 \pmod{g(x)},$$

где $L = \{a_1, a_2, \dots, a_{2n}\}$, $a_i \in GF(q^m)$ и $g(x)$ - многочлен с коэффициентами из $GF(q^m)$, не имеющий среди своих корней элементов из L , то есть $g(a_i) \neq 0$, $q^m > n$ и t - простое или степень простого числа. Для выполнения процедуры кодирования используется порождающая матрица кода G . То есть, чтобы получить кодовое слово (n, k) - кода, соответствующее некоторому информационному сообщению $P = (P_1, P_2, \dots, P_k)$, достаточно умножить вектор p на порождающую матрицу кода G .

Для построения порождающей матрицы (L, g) - кода сначала необходимо построить проверочную матрицу H , используя множество L и многочлен $g(x)$.

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \\ \dots & \dots & \dots & \dots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \dots & \alpha_n^{t-1} \\ g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \end{pmatrix},$$

где $t = \deg g(x)$.

Имея проверочную матрицу H , легко построить порождающую матрицу кода G : $GH^T = 0$, используя метод Гаусса приведения матрицы H к диагональному виду. Для получения матрицы, обеспечивающей шифрующее преобразование, необходимо дополнительно выбрать две матрицы. Произвольную не особую (имеющую обратную) матрицу A размера $k \times k$ и произвольную перестановочную матрицу P размера $n \times n$.

Таким образом, шифруемая информация будет разбиваться на двоичные блоки $p = (p_1, p_2, \dots, p_k)$ длины k и подвергаться следующему преобразованию:

$$C = p \cdot A \cdot G \cdot P + e,$$

где A – неособенная (обратимая) матрица $(k \times k)$,

G – порождающая матрица кода Гоппы $(k \times n)$,

P – произвольная перестановочная матрица $(n \times n)$,

E – случайный вектор ошибки веса $t/2$.

Алгоритм декодирования-дешифрации выглядит следующим образом:

1. Принятое сообщение умножается на матрицу P^{-1} обратную к перестановочной матрице P :

$$c \cdot P^{-1} = (p \cdot A \cdot G \cdot P \oplus e) \cdot P^{-1} = p \cdot A \cdot G \cdot P \cdot P^{-1} \oplus e \cdot P^{-1} = p \cdot A \cdot G \oplus e \cdot P^{-1} = p' \cdot G \oplus e',$$

где $p' = p \cdot A$ – измененное информационное сообщение,

$e' = e \cdot P^{-1}$ – случайный вектор ошибки веса $t/2$.

2. Таким образом, получится кодовое слово (L, g) -кода, сложенное со случайным вектором ошибки. Зная многочлен Гоппы $g(x)$ и множество локаторов позиций, можно найти и исправить вектор ошибок e' , используя конструктивный алгоритм декодирования (Берликэмп-Мэсси, Евклида).

3. Зная порождающую матрицу кода G и матрицу A , легко восстановить сначала измененное информационное сообщение p' , а затем – и исходное информационное сообщение p :

$$p' \cdot A^{-1} = p \cdot A \cdot A^{-1} = p$$

7.2. Модификация схемы МакЭлиса для шифрации видеоизображения

Для эффективного использования описанной схемы необходимо выбрать параметры (L, g) -кода, обеспечивающие эффективную обработку исходной информации и достаточный уровень защищенности. Как известно, защищенность такой схемы, даже в случае разглашения информации о параметрах кода (длина кодового слова, 101 длина информационного сообщения и число исправляемых ошибок), определяется числом различных многочленов Гоппы степени t :

$$N = O\left(\frac{q^t}{t}\right),$$

где коэффициенты многочленов Гоппы выбираются из поля $GF(q)$.

Например, при выборе двоичного кода (256, 128, 33) с многочленом Гоппы степени 16 и коэффициентами из $GF(2^8)$ мы получим систему, защищенность которой будет оцениваться величиной $O(2^{124})$.

На предающем (шифрующем) устройстве имеется лишь информация об открытом ключе (матрица $G' = A \cdot G \cdot P$ и генератор ошибок заданного веса t). Получение информации о шифрующей матрице не позволяет определить многочлен Гоппы, а, следовательно, не дает возможности исправлять случайные ошибки, «накладываемые» на передаваемое изображение. Использование такого алгоритма обработки видеоизображения позволяет решить сразу две задачи: – нет необходимости синхронизировать приемное и передающее устройство (зная многочлен Гоппы на приемном устройстве всегда можно исправить любые ошибки веса до t), – передающее устройство не содержит конфиденциальной информации, и его компрометация не позволяет правильно декодировать искаженное видеоизображение. Следует отметить, что особенностью шифрования видеоизображения является наличие довольно большого числа информационных блоков, имеющих одно и то же значение (фоновые текстуры, контуры и т.д.). Для обеспечения преобразования совпадающих информационных блоков в различные зашифрованные сообщения в рассмотренном выше алгоритме используются вектора 102 ошибок веса до t . Однако, при наличии достаточного числа (больше трех) одинаковых информационных блоков можно использовать мажоритарный метод исправления ошибок. Для предотвращения такой атаки можно использовать сгенерированный случайный вектор ошибки для «искажения» значения информационного блока. Легко оценить число таких возможных «искажений» – K :

$$K = \binom{n}{t}$$

Рассмотрим некоторые способы «искажения» информационного сообщения, аналогичные используемым в схеме МакЭлиса для «искажения» кодового слова. Схема Rao-Nam предполагает использование для этой цели специального, заранее выбранного кодового слова из общего списка кодовых слов. То есть для каждого вектора ошибки, являющегося лидером смежного класса в таблице стандартной расстановки кода, выбирается соответствующее кодовое слово, список таких кодовых слов является элементом секретного ключа. Процедура шифрования в соответствии со схемой Rao-Nam выглядит следующим образом:

$$c = p \cdot G' \oplus e' \cdot P,$$

где $e' = e \oplus 1, l$ – кодовое слово, соответствующее вектору ошибки:

$$wt(e) \leq t, G' = A \cdot G.$$

Очевидно, что эта процедура может быть переписана в следующем виде:

$$c = (p \oplus \lambda) \cdot G' \oplus e \cdot P,$$

где λ - информационное сообщение, соответствующее кодовому слову l : $l = \lambda \cdot A \cdot G$.

Очевидным недостатком данной схемы является необходимость хранить кодовые слова $\{1\}$ или информационные сообщения $\{t\}$, 103 соответствующие всем лидерам смежных классов, как на приемной, так и на передающей стороне. Второй известной модификацией схемы МакЭлиса является схема, предложенная в работах и использующая структуру схемы Эль Гамала. В этой схеме зашифрованное сообщение состоит из трех частей c_1 , c_2 , c_3 и получается следующим образом:

$$c_1 = p \cdot (G' \oplus S_m \cdot D_m) \oplus e \cdot (P \cdot X \oplus S_e \cdot D_e),$$

где e - случайный вектор ошибки длины n , $wt(e) < t$,

$G' = A \cdot G \cdot X$, X - несингулярная матрица $n \times n$,

S_m - случайная матрица $k \times m$,

D_m - случайная матрица $n \times n$,

P - случайная перестановочная матрица $n \times n$,

S_e - случайная матрица $k \times n$,

D_e - случайная матрица $n \times n$,

$C_2 = e \cdot S_e$,

$C_3 = p \cdot S_m$,

$C = c_1 \parallel c_2 \parallel c_3$.

Открытым ключом, используемым на передающей стороне для преобразования исходной информации p , являются матрицы:

$$G' \oplus S_m \cdot D_m, P \cdot X \oplus S_e \cdot D_e, S_e, S_m.$$

С точки зрения решаемой нами задачи - уничтожения структуры видеоизображения - данная схема оказывается неприемлемой из-за наличия в каждом зашифрованном сообщении компоненты c_3 , которая будет иметь одинаковые значения для одинаковых исходных сообщений, то есть одинаковые фрагменты изображения могут быть легко распознаны по этой компоненте. Третьим вариантом, также имеющим структуру схемы Эль Гамала, является вариант схемы МакЭлиса, предложенный в работе. Здесь 104 так же, как и в предыдущем случае, зашифрованное сообщение состоит из трех компонент c_1 , c_2 , c_3 и получается следующим образом:

$$c_1 = (c_1^1, c_1^2, \dots, c_1^i, \dots, c_1^k), c_1^i = p_i \cdot \beta_i \bmod q,$$

где β_i – случайные числа из $GF(q)$.

$$c_2 = \begin{bmatrix} \beta_1 & 0 & 0 & \dots & 0 \\ 0 & \beta_2 & 0 & \dots & 0 \\ 0 & 0 & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & \beta_k \end{bmatrix} \cdot (G' \oplus R') \oplus E \cdot P'$$

где E – случайная матрица $n \times n$ над $GF(q)$, каждая строка которой имеет не более t не нулевых элементов,

R' – случайная матрица $k \times n$ с элементами из $GF(q)$,

P' – случайная перестановочная матрица $n \times n$ с элементами из $GF(q)$,

G' , R' и P' – матрицы, составляющие открытый ключ,

$$c_3 = T \cdot G' \oplus E,$$

где T – произвольная матрица $k \times k$ с элементами из $GF(q)$.

Очевидно, что такой вариант модификации схемы МакЭлиса в большей степени подходит для решения нашей задачи – разрушения структуры изображения, однако основным недостатком данной схемы является более чем трехкратное увеличение объема передаваемой информации. В данной работе для решения поставленной задачи предлагается некоторая модификация схемы Rao-Nam для обеспечения повышения информационной скорости передачи информации и скрытности. Использование такой модификации позволяет избежать хранения массива кодовых слов на передающей и приемной стороне для их использования в качестве 105 секретного ключа. Вместо хранения такого массива предлагается использовать некоторое преобразование вектора e длины n в вектор f длины k . Простейшим и эффективным вариантом такого преобразования может быть хэш-функция. То есть предлагаемая схема может быть описана следующим образом:

$$c = (p \oplus f) \cdot G' + e \cdot P,$$

где $f = \text{hash}(e)$.

Описанный выше метод используется для повышения информационной скорости передачи зашифрованных данных. Для решения рассматриваемой задачи – максимального изменения структуры изображения – возможно также использование случайных чисел, генерируемых в виде векторов ошибки e , $\text{wt}(e) < t$ для создания случайной несингулярной матрицы

A^* размерности $k \times k$: $f: e \rightarrow A^*$. Полученную матрицу A^* можно использовать для преобразования исходной информации следующим образом:

$$c = p \cdot G^* + e \cdot P,$$

Для рассмотренного выше примера (256, 128, 33) кода Гоппы число возможных различных векторов ошибки веса 16 составляет величину $0(28\ 2)$, и соответственно каждый из $21\ 2\ 8$ информационных векторов может быть преобразован с помощью случайного вектора f или матрицы A^* в один из $28\ 2$ возможных случайных информационных векторов. Очевидно, что такая модификация схемы МакЭлиса позволяет избежать преобразования одинаковых фрагментов видеоизображения в малоотличающиеся (не более чем в $2t$ позициях), зашифрованные сообщения.

7.3. Пример использования модифицированной схемы МакЭлиса

Пример работы рассмотренной системы для цветного изображения при выбранных параметрах кода изображен на рис. 33.



Рис. 33. Результат применения модифицированной схемы МакЭлиса для цветного изображения

Более сложный случай – монохромные, высококонтрастные изображения. Исходное и маскированное изображения приведены на рис. 34.

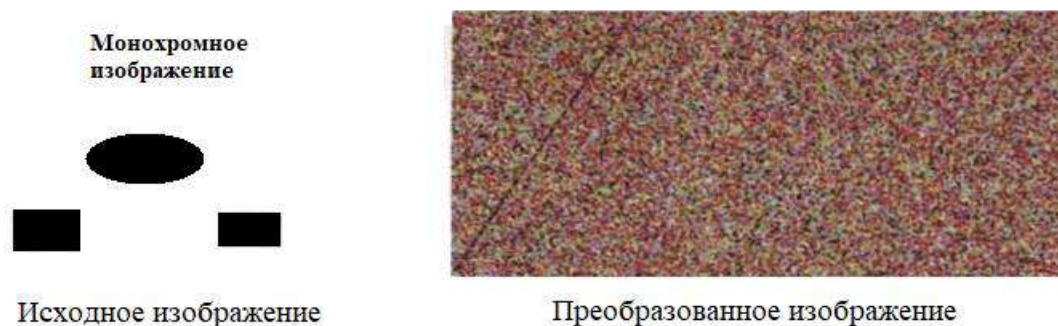


Рис. 34. Результат применения модифицированной схемы МакЭлиса для монохромного изображения

Заключение

Свобода проявлений себя в информационном пространстве позволяет преступным элементам действовать дерзко и безбоязненно, в связи с чем возможно утверждать, что информатизация общества, обладая, несомненно, множеством позитивных качеств, привела и к информатизации криминальной среды, придала ей ярко выраженный интернациональный и высокотехнологичный характер. Лица, склонные к совершению вышеуказанных преступлений, используют возможности информационно-телекоммуникационных систем, что способствует расширению транснационального масштаба преступности, и, как результат, в конечном итоге определяют и создают угрозу национальной безопасности³⁴.

На протяжении многих лет сотрудники органов внутренних дел ведут упорную борьбу, направленную на своевременное предупреждение, выявление, раскрытие и успешное расследование преступлений, совершаемых в условиях цифровизации с использованием, в зависимости от возникшей ситуации (оперативно-розыскной, следственной или криминалистической), всех необходимых возможностей информационно-коммуникационных технологий.

Зачастую данный вид преступлений носит латентный характер. Способы совершения рассматриваемых преступлений постоянно видоизменяются, в механизм совершения преступлений вносятся новые ухищрения, в связи с чем раскрытие указанных преступлений становится затруднительным. Такое положение требует от сотрудников правоохранительных органов необходимого получения специальных знаний, умений и навыков в указанной сфере, что окажет положительное влияние на своевременное осуществление противодействия преступлениям, подготавливаемым или уже совершенным в условиях цифровизации.

Для решения данной задачи необходимо постоянно вести активную работу по подготовке учебно-методических материалов с освещением практического опыта раскрытия рассматриваемых видов преступлений, что благоприятно будет сказываться на профессиональных компетенциях сотрудников органов внутренних дел.

Преступления, совершаемые в сфере телекоммуникаций и компьютерной информации, в абсолютном большинстве случаев носят корыстный характер. Все чаще мы сталкиваемся с таким распространенным видом преступлений, как мошенничество, которое в настоящее время практически каждый день совершается разными изощренными способами.

Преступления, совершаемые в этой сфере, позволяют преступникам анонимизироваться. Высокая степень анонимности, обеспечиваемая воз-

³⁴ Алескеров В.И., Баранов В.В. Телекоммуникация и киберпространство как средство преступлений экстремистской и террористической направленности//Труды Академии управления МВД России. 2020, №1 (53). С. 104-113.

возможностями глобальной сети Интернет, может существенно облегчить обман предполагаемой жертвы и последующее завладение ее имуществом.

Выбор именно этой разновидности преступлений обусловлен широким распространением мошенничества, многообразием способов его совершения и другими факторами. Мошенники всегда имеют желание максимально обогатиться в минимальные сроки и без финансовых затрат. В связи с этим единственно верным выходом из такой ситуации будет своевременное, постоянное, максимально полное и эффективное информирование о предполагаемой опасности быть обманутым. Данное информирование должно проходить в рамках правоохранительной деятельности наряду:

- с эффективным проведением профилактической работы, направленной на предупреждение рассматриваемой категории преступлений;
- со своевременным выявлением преступлений;
- с качественным расследованием преступлений;
- с постоянным информированием населения о результатах деятельности правоохранительных органов по предупреждению и недопущению преступлений;
- с постоянной работой, направленной на более эффективное сотрудничество со средствами массовой информации.

Результаты такой деятельности обеспечат пользователям максимальную безопасность в глобальной сети Интернет.

Информационная среда, в том числе и глобальная сеть Интернет, является сложной технологической системой. Раскрытие преступления как факта его совершения и дальнейшее успешное расследование преступлений в сети Интернет требует от субъекта расследования не только юридических, но и обширных специальных знаний в области информационно-телекоммуникационных технологий, а также новых алгоритмов действий сотрудников органов внутренних дел, направленных на осуществление своевременного противодействия в рамках правового поля.

Предотвращение, пресечение и раскрытие данного вида преступлений всегда зависит от своевременно полученной информации, способа совершения преступления, профессионализма сотрудников и тесного взаимодействия структурных подразделений Министерства внутренних дел Российской Федерации с другими правоохранительными органами и ведомствами.

Одновременно с высокими темпами развития общества и расширением сфер его жизнедеятельности все большее внимание уделяется использованию возможностей сферы телекоммуникаций и компьютерной информации. Количество пользователей этой сферы растет с каждым годом, в связи с чем возникают и проблемы, которые носят циклический характер, что создает благоприятную основу для совершения новых видов преступлений.

В настоящее время, на наш взгляд, можно выделить следующие основные проблемы, связанные с расследованием различных видов

преступлений, совершаемых с использованием возможностей глобальной сети Интернет:

1. Недостаточно высокая квалификация лиц, занимающихся расследованием данных преступлений.

2. Недостаток практики расследования некоторых видов интернет-мошенничеств.

3. Относительно большое количество преступлений, остающихся нераскрытыми.

4. Недостаточное количество комментариев специалистов на актуальные проблемные вопросы расследования мошенничеств, совершенных с использованием сети Интернет.

Исходя из выше изложенного, можно сказать, что борьба с мошенничеством, совершаемым с использованием сферы телекоммуникаций и компьютерной информации, в условиях цифровизации с каждым днем все более усложняется. Возникающие оперативно-розыскные и следственные ситуации требуют от должностных лиц высокого профессионализма. Для разрешения этих обстоятельств требуется серьезный подход, и имеющаяся статистика о раскрытии данных видов преступлений говорит о том, что сотрудники органов внутренних дел с ними успешно справляются.

Все чаще через средства массовой информации населению доводятся сведения о новых способах совершения современных видов преступлений организованными преступными группами в условиях цифровизации и причиненном ущербе. Данная профилактическая работа положительно сказывается на отношении населения к использованию возможностей современных информационных технологий. Однако еще имеют место быть такие факты, как проявление доверия наших граждан на используемые способы-уловки со стороны преступников. Злоумышленники, совершая преступления с использованием возможностей IT-технологий в условиях цифровизации, с каждым днем придумывают все новые ситуации, в которых проводят диалог со своими будущими жертвами, и, таким образом, достигают путем метода глубокого убеждения и оказанного психологического давления на будущих жертв-потерпевших своего преступного замысла – необходимого результата.

Помимо рассматриваемого вида преступлений такого, как мошенничество, набирают обороты и преступления, совершаемые в системе дистанционного банковского обслуживания.

Анализируя и обсуждая актуальные вопросы, наиболее часто встречающиеся в ходе своевременного раскрытия и дальнейшего успешного расследования преступлений, совершаемых в системе дистанционного банковского обслуживания, необходимо сотрудникам оперативных подразделений и следственных органов:

1. Постоянно повышать свой уровень профессиональных знаний, касающихся непосредственных особенностей организационного, технического и правового обеспечения раскрытия и расследования преступлений.

2. Постоянно изучать не только нормы уголовного права, уголовного процесса, оперативно-розыскной деятельности, новейшие достижения науки криминалистики, но и других смежных наук, дающие ответы на сложные вопросы, возникающие в ходе раскрытия рассматриваемой категории преступлений.

3. Постоянно быть в курсе последних нововведений и положений, отраженных в законодательстве банковского, гражданского, информационного, корпоративного права и других смежных отраслей знаний.

4. Своевременно получать информацию об организации и технологии обеспечения ДБО, что положительно будет способствовать раскрытию преступлений, совершаемых в системе ДБО.

5. С целью недопущения пробелов в работе постоянно изучать положения решений Пленумов Верховного Суда Российской Федерации о практике рассмотрения уголовных дел по фактам хищения денежных средств в системе ДБО для получения полной информации о ситуации, складывающейся в настоящее время.

6. Все большее внимание уделять взаимодействию между регионами Российской Федерации, а также с зарубежными государствами по раскрытию преступлений, совершаемых в системе ДБО.

7. Активизировать целенаправленную работу по своевременному выявлению лиц и организованных преступных групп, склонных к совершению преступлений террористического характера и экстремистской направленности, которые все чаще используют возможности современных информационно-коммуникационных технологий.

8. Рассматриваемые виды преступлений в большинстве случаев имеют транснациональный характер. Зачастую, они начинаются в одном регионе того или иного государства, имеют свое продолжение в другой стране, а заканчиваются в третьей. В этих ситуациях разоблачение организованной преступной группы становится более проблематичным. Одной из таких проблем являются различия в национальных уголовных и уголовно-процессуальных законодательствах тех или иных зарубежных государств, что препятствует привлечению к уголовной ответственности лиц, причастных к совершению преступлений.

В связи с изложенным необходимо принять неотложные меры по урегулированию законодательства в сфере противодействия преступлениям, совершаемым с использованием возможностей телекоммуникаций и компьютерной информации, на международном уровне.

Предложенные меры и сделанные выводы по ключевым вопросам раскрытия и расследования преступлений в информационно-коммуникационном пространстве, по нашему мнению, окажут существенную помощь в борьбе с современными видами преступлений, совершаемыми в условиях цифровизации.

В настоящее время в связи с развитием информационных технологий преступники продумывают и внедряют все более продвинутые системы перехвата и дешифровки информации, что может даже повлечь за собой кражу оперативно значимой информации, вырабатываемой в процессе проведения оперативно-розыскных мероприятий компетентными государственными органами и сотрудниками правоохранительной системы Российской Федерации.

Представленное научно-практическое пособие позволит сотрудникам органов внутренних дел, призванным по своим функциональным обязанностям предотвращать, пресекать, своевременно раскрывать и качественно расследовать преступления, совершаемые в информационно-коммуникационной среде, в достаточном объеме иметь представление о складывающейся криминальной обстановке. Собранные наработки, взятые из практической деятельности сотрудников правоохранительных органов Российской Федерации, касающиеся отечественного и зарубежного опыта борьбы с преступлениями, совершаемыми в условиях цифровизации, будут способствовать эффективному раскрытию преступлений данного вида.

Также в данной работе представлен актуальный на сегодняшний день практический опыт по защите видеоинформации, который, в свою очередь, может способствовать предотвращению перехвата, модификации, уничтожения и препятствованию доступа к оперативно значимой информации, вырабатываемой оперативными сотрудниками органов внутренних дел Российской Федерации.

Авторский коллектив научно-практического пособия выражает свою глубокую признательность и благодарность в оказании помощи по сбору материалов сотрудникам территориальных подразделений специальных технических мероприятий органов внутренних дел, Академии управления МВД России, а также слушателям, проходившим в разные периоды обучение на кафедре оперативно-технических мероприятий органов внутренних дел Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации.



Литература

1. **Российская Федерация. Законы.** Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с изм., одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 28.05.2026).

2. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ. // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 28.05.2026).

3. **Российская Федерация. Законы.** Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18 декабря 2001 г. № 174-ФЗ (ред. от 10 июня 2026 г.) // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 15.06.2026).

4. **Российская Федерация. Законы.** Гражданский кодекс Российской Федерации : Федеральный закон от 30 ноября 1994 г. № 51-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 06.06.2026).

5. **Российская Федерация. Законы.** О государственной тайне : Закон Российской Федерации от 21 июля 1993 г. № 5485-1 // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_2481/ (дата обращения: 02.06.2026).

6. **Российская Федерация. Законы.** Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 29.05.2026).

7. **Российская Федерация. Законы.** О Центральном банке Российской Федерации (Банке России) : Федеральный закон от 10 июля 2002 г. № 86-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL:

https://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 23.06.2026).

8. Российская Федерация. Законы. О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 15.06.2026).

9. Российская Федерация. Законы. О коммерческой тайне : Федеральный закон от 29 июля 2004 г. № 98-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 18.06.2026).

10. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 29.05.2026).

11. Российская Федерация. Президент. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы : Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Информационно-правовой портал «Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/71570570/> (дата обращения: 29.05.2026).

12. Российская Федерация. Правительство. Об утверждении Положения о защите информации в платежной системе : постановление Правительства Российской Федерации от 13 июня 2012 г. № 584 // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_131173.05c3fl053d0d0a27e491cc7c3a0d509157c92a4f/ (дата обращения: 05.06.2026).

13. Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств : указание Банка России от 9 июня 2012 г. № 2831-У // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_131471/251f7ac207ca304c6331640eb36b162351c24684/ (дата обращения: 05.06.2026).

14. О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности : письмо Банка России от 24 марта 2014 г. № 49-т // Информационно-правовой портал

«Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/70526030/> (дата обращения: 05.06.2026).

15. **Российская Федерация.** Об утверждении типовых Требований к плану мероприятий по внедрению технических средств, обеспечивающих оперативно-розыскную деятельность : приказ Минцифры России, ФСБ России от 28 марта 2022 г. № 245/127 // Информационно-правовой портал «Гарант.Ру». – URL: <https://www.garant.ru/products/ipo/prime/doc/404991787/> (дата обращения: 10.06.2026).

16. **Российская Федерация.** Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : приказ МВД России, МО России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 // Информационно-правовое обеспечение «Гарант» : [сайт]. – URL: <https://base.garant.ru/70531824/> (дата обращения: 15.06.2026).

17. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – Москва : Госстандарт СССР, 1989.

18. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. – Москва : Госстандарт России, 1994.

19. Состояние преступности за 2010-2025 гг. : сборники ФКУ «ГИАЦ МВД России».

20. **Акопов, Г. Л.** Интернет и политика. Модернизация политической системы на основе инновационных политических интернет-коммуникаций / Г. Л. Акопов. – Москва : Кнорус, 2014.

21. **Алескеров, В. И.** Уголовно-правовая и криминалистическая характеристика современных видов преступлений в сфере компьютерной информации : лекция / В. И. Алескеров, И. А. Максименко. – Домодедово : ВИПК МВД России, 2011.

22. **Алескеров, В. И.** Преступления, совершаемые в телекоммуникационных сетях, как разновидность преступлений в сфере компьютерной информации : аналитический сборник / В. И. Алескеров, Ф. А. Куц. – Домодедово : ВИПК МВД России, 2014.

23. **Алескеров, В. И.** Особенности раскрытия преступлений в сфере компьютерной информации : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова. – Домодедово : ВИПК МВД России, 2015.

24. **Алескеров, В. И.** Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова. – Домодедово : ВИПК МВД России, 2018.

25. **Алескеров, В. И.** Выявление и раскрытие преступлений экстремистской и террористической направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, А. И. Федоткин. – Домодедово : ВИПК МВД России, 2018.

26. **Алескеров, В. И.** Раскрытие преступлений в системе дистанционного банковского обслуживания : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко. – Домодедово : ВИПК МВД России, 2020.

27. **Алескеров, В. И.** Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко. – Домодедово : ВИПК МВД России, 2022.

28. **Алескеров, В. И.** Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко; под общ. ред. М. Ю. Литвинова. – Домодедово : ВИПК МВД России, 2024.

29. **Алескеров, В. И.** Раскрытие дистанционных хищений, совершаемых с использованием IT-технологий : научно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Е. В. Маркелова [и др.]; под общ. ред. М. Ю. Литвинова. – Домодедово : ВИПК МВД России, 2024.

30. **Литвинов, М. Ю.** Противодействие современным видам преступлений, совершаемых в условиях цифровизации : учебно-практическое пособие : в 3 частях / М. Ю. Литвинов, В. И. Алескеров, О. Н. Колокольчикова. – Домодедово : ВИПК МВД России, 2025.

31. **Алпатов, А. С.** Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием / А. С. Алпатов // Трибуна молодого ученого. – 2016. – № 2.

32. **Баулин, В. В.** Методы совершения хищений денежных средств через систему дистанционного банковского обслуживания / В. В. Баулин, Д. Волков, В. В. Баранов, А. А. Рыжков // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». – Москва, 2014.

33. **Брюс Шнайер.** Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си, ред. П. В. Семьянов. – Москва : Триумф, 2002.

34. **Беззатеев, С. В.** Использование помехоустойчивых кодов для шифрации видеоинформации / С. В. Беззатеев, М. Ю. Литвинов, Б. К. Трояновский // Информационно-управляющие системы. – 2004. – № 5(30).

35. **Беззатеев, С. В.** Выбор алгоритма преобразования, обеспечивающего изменение структуры изображения / С. В. Беззатеев, М. Ю. Литвинов, Б. К. Трояновский [и др.]. // Информационно-управляющие системы. – 2006. – № 6 (25).

36. **Винокуров, А.** Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86. – URL: <http://www.cybersecurity.ru/manuals/crypto/ssl/780.html>.

37. **Винокуров, А.** Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США, «Системы безопасности» / А. Винокуров, Э. Применко. – Москва : Изд. «Гротэк», 2001, № 1, № 2.

38. **Винокуров, А.** Как устроен блочный шифр? // URL: www.itim.by/grodno/index.php, Филиал Института технологий информатизации и управления БГУ (г. Гродно).

39. **Гоппа, В. Д.** Новый класс линейных помехоустойчивых кодов // Проблемы передачи информации. – 1970. – Т. 6, № 3.

40. **Дуленко, В. А.** Преступление в сфере высоких технологий: учебное пособие / В. А. Дуленко, Р. Р. Мамлеев, В. А. Пестриков. – Москва : ЦОКР МВД России, 2010.

41. **Еферин, В. П.** Организация деятельности территориальных органов МВД России на районном уровне по противодействию терроризму и экстремизму : учебное пособие / В. П. Еферин, Ю. П. Хорькин. – Домодедово : ВИПК МВД России, 2014.

42. Историческая и социально-образовательная мысль // Всероссийский научный журнал. – 2014. – № 4 (26).

43. Комментарий к Уголовному кодексу Российской Федерации (постатейный) (14-е издание, переработанное и дополненное) / отв. ред. А.И. Рарог. – «Проспект», 2023.

44. **Кочои, С.** Ответственность за неправомерный доступ к компьютерной информации / С. Кочои, Д. Савельев // Российская юстиция. – 1999. – № 1.

45. Криптографическая защита информации : учебное пособие / А. В. Яковлев, А. А. Безбогов, В. В. Родин [и др.]. – Тамбов : Изд-во ТГТУ, 2006.

46. **Крылов, В. В.** Информация как элемент криминальной деятельности / В. В. Крылов // Российская юстиция. – 2000. – № 5.

47. **Литвинов, М. Ю.** О проблемах реализации защищенного обмена видеоданными в современных распределенных системах / М. Ю. Литвинов, Г. П. Филатов, М. Б. Сергеев // Известия СПб ГЭТУ (ЛЭТИ). Серия «Биотехнические системы в медицине и биологии». – 2006. – Выпуск 2.

48. **Литвинов, М. Ю.** Совмещение растровых изображений в системах технического зрения / М. Ю. Литвинов, Н. В. Соловьев, А. А. Козлов // Информационно-управляющие системы. – 2007. – № 6(31).

49. **Лукашов, И.** Аппаратные шифраторы на отечественной элементной базе : ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2001. – № 6.

50. **Маторин, М. А.** Актуальные вопросы формирования правовой системы противодействия терроризму / М. А. Маторин // Оперативник (сыщик). – 2014. – № 2 (39).

51. **Медведев, В. Н.** Правовое регулирование снятия информации с технических каналов связи в оперативно-розыскной деятельности : диссертация ... кандидата юридических наук. – Санкт-Петербург : Санкт-Петербургский университет, 2003.

52. **Мельников, Д. А.** Организация и обеспечение безопасности информационно-телекоммуникационных сетей и систем : учебник / Д. А. Мельников. – Москва : ИД КДУ, 2015.

53. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов [и др.] / Диалог-МИФИ, 2002.

54. **Мирошников, Б. Н.** Сетевой фактор. Интернет и общество / Б. Н. Мирошников. – Москва : Кучково поле, 2015.

55. **Россинская, Е. Р.** Судебная экспертиза в гражданском, административном и уголовном процессе / Е. Р. Россинская. – Москва : Норма, 2020.
56. Сайт Центра исследований компьютерной преступности. – URL: <http://www.crime-research.ru> (дата обращения: 20.01.2018).
57. **Санкин, П. С.** Особенности оценки содержимого сжатого видеопотока / П. С. Санкин, М. Ю. Литвинов // Информационно-управляющие системы. – 2009. – № 3.
58. **Сейджман, М.** Сетевые структуры терроризма / М. Сейджман. – Москва : Идея-Пресс, 2008.
59. **Синякин, И. И.** Терроризм с использованием оружия массового уничтожения: международно-правовые вопросы противодействия : монография / И. И. Синякин. – Москва : Норма, 2012.
60. **Сорокин, А. В.** Судебная практика по делам о преступлениях в сфере компьютерной информации / А. В. Сорокин. – URL: http://www.zaural.ru/procur/my_page.htm (дата обращения: 20.01.2021).
61. Теория оперативно-розыскной деятельности : учебник. – 3-е изд., перераб. и доп. / под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. – Москва : ИНФРА-М, 2014.
62. Терроризм в современном мире. – 2-е изд. / под ред. В. Л. Шульца; Центр исследования проблем безопасности РАН. – Москва : Наука, 2011.
63. **Тищенко, В. И.** Сетевые взаимодействия. Предмет исследования и объект моделирования / В.И. Тищенко, Т.И. Жуков, Ю.С. Попков. – Москва : Ленанд, 2014. – 352 с.
64. **Ткаченко, В. В.** Российский терроризм. Проблемы уголовной ответственности : монография / В.В. Ткаченко. – Москва : ИНФРА-М, 2014.
65. **Троицкий, С. В.** Международно-правовые формы сотрудничества государств по противодействию терроризму / С.В. Троицкий // Государство и право. – 2014. – № 2.
66. **Ульянова, В. В.** Проблемы реализации уголовной ответственности за содействие террористической деятельности в форме финансирования терроризма / В.В. Ульянова // Актуальные проблемы российского права. – 2014. – № 3.
67. **Фам Суан Нгиа.** Модификации алгоритма МакЭлис для повышения показателей качества радиосистем передачи информации : диссертация ... кандидата технических наук: спец. 05.12.04. – Рязань : Рязанский государственный радиотехнический университет, 2007.

68. **Фатьянов, А. А.** Правовое обеспечение безопасности информации в Российской Федерации : учебное пособие / А. А. Фатьянов. – Москва : 2001.

69. **Чекунов, И. Г.** Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И. Г. Чекунов // Право и кибербезопасность. – 2012. – № 1.

70. **Шаталов, А. С.** Криминалистические алгоритмы и программы. Теория. Проблемы. Прикладные аспекты / А. С. Шаталов. – Москва : Лига Разум, 2000.

71. **Шаталов, А. С.** Уголовно-процессуальное право Российской Федерации : академический курс по направлению «Юриспруденция» / А. С. Шаталов, А. А. Крымов. – Москва : Проспект, 2018.

72. **Шаталов, А. С.** Уголовно-процессуальный кодекс Российской Федерации в схемах: учебное пособие / А. С. Шаталов. – Москва : Проспект, 2021.

73. **Шеннон, К.** Работы по теории информации и кибернетике / К. Шеннон. – Москва : 1963.

74. **Шмонин, А. В.** Организация выявления и раскрытия хищений денежных средств с использованием дистанционного банковского обслуживания / А. В. Шмонин // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». – Москва, 2014.

75. CCITTRec.T.81 (1992 E) | ISO/IEC 10918-1: 1993(E). Information technology - Digital compression and coding of continuous-tone still images: Requirements and guidelines.

76. ISO/IEC 13818-2:2000 Information technology - Generic coding of moving pictures and associated audio information.

77. Р 78.36.002-99 «Выбор и применение телевизионных систем видеоконтроля. Рекомендации» НИЦ «Охрана» ГУВО МВД России, 1999.

78. Agi, Li Gong An Empirical Study of Secure MPEG Video Transmission. In Proceedings of the Internet Society Symposium on Network and Distributed System Security // Symposium on Network and Distributed System Security. February 22-23, 1996 / San Diego Princess Resort, San Diego, California.

79. Lei Tang Methods for encrypting and decrypting MPEG data efficiently // International Multimedia Conference Proceedings of the fourth ACM international conference on Multimedia / Boston, Massachusetts, USA, 1997.

80. Bharat Bhargava, Changgui Shi, Sheng-Yih Wang. MPEG Video Encryption Algorithms // Computer Communications, 2005, vol. 28, № 6.
81. Lintian Qiao, Klara Nahrstedt. Comparison of MPEG encryption algorithms // Computers & Graphics, 1998, vol. 22, № 4.
82. Liu X., Eskicioglu A.M. Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions // Communications, Internet, and Information Technology (CUT 2003) Scottsdale, AZ, USA. Nov. 17- 19, 2003.
83. O. Chung-Ping Wu, C-C Jay Cuo. Efficient multimedia encryption via entropy codec design // Proceedings of SPIE Volume 4314 - Security and Watermarking of Multimedia Contents III, (San Jose, CA, USA), Jan. 2001.
84. Marc Van Droogenbroeck and Raphaël Benedett. Techniques for A Selective Encryption Of Uncompressed And Compressed Images // Proceeding of ACIVS (Advanced Concepts for Intelligent Vision Systems) Ghent, Belgium, September 9- 11, 2002.
85. Martina Podesser, Hans-Peter Schmidt, Andreas Uhl. Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments // IEEE Transactions on Signal Processing, 43(3), March 1995.
86. Tanya E. Seidel, Daniel Socek, Michal Sramka. Cryptanalysis of Video Encryption Algorithms // The 3rd Central European Conference on Cryptology (TATRACRYPT 2003) June 26 - 28, 2003.
87. Shujun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo. On the Design of Perceptual MPEG-Video Encryption Algorithms // CoRR, 2005, vol. 28, № 6.
88. AH S, Aman Tosun, Wu-chi Feng. On Error Preserving Encryption Algorithms for Wireless Video Transmission // ACM Multimedia, 2001.
89. Daniel Socek, Spyros Magliveras, Dubravko Culibrk, Oge Marques, Hari Kalva, Borko Furht. Permutation-Based Correlation-Preserving Encryption Method for Digital Videos // EURASIP Journal on Information Security Volume 2007 (2007), Article ID 52965.
90. Biryukov A., Wagner D. Advanced Slide Attacks., <http://citeseer.ist.psu.edu> - 2000.
91. John Kelsey, Bruce Schneier, David Wagner, Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES // Advances in Cryptology - CRYPTO '96 Proceedings, Springer-Verlag, August 1996.
92. FIPS 180-1. SECURE HASH STANDARD.
93. FIPS 180-2. Secure Hash Signature Standard (SHS).

94. Florian Mendel, Norbert Pramstaller Cryptanalysis of the GOST Hash Function // ASIACRYPT, 2007.
95. Schneier on Security: New Cryptanalytic Results Against SHA-1 // [http ://www. schneier. com/](http://www.schneier.com/).
96. Beginning Cryptography with Java, [http ://www. auto chthonous. org/crypto/](http://www.autochthonous.org/crypto/).
97. Mitsum Matsui «Linear Cryptanalysis Method for DES Cipher» // Advances in Cryptology: EUROCRYPT '93, T. Helleseht, editor. Lecture Notes in Computer Science, vol. 765, Springer-Verlag, Berlin, 1994.
98. Biham Eli, Shamir Adi Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993.
99. John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting Improved Cryptanalysis of Rijndael // Fast Software Encryption: 7th International Workshop, Fse 2000, New York, Ny, Usa, April 10-12, 2000.
100. McEliece R.J. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report, Jet Propulsion Laboratory, Pasadena, CA, Jan/Feb, 1978.
101. T.R.N.Rao, Kil-Myun Nam, Private-key algebraic-code encryptions, IEEE Trans, on Information Theory, vol.35, no. 4, 1989.
102. Krouk E. A new public-key cryptosystem // Proceedings of the 6-th Joint Swedish-Russian International Workshop on Information Theory, 1993.
103. Gabidulin E.M. Public-key cryptosystem based on linear codes // Designs, Codes and Cryptography, № 6(1), 1995.
104. Jian-feng M.A, Chiam Teechye, Kot Chichung Alex, A novel encryption method with its application in the copyright protection of digital data, Journal of Software, vol. 13, № 3, 2002.
105. Bezzateev S.V., Litvinov M.Y, Krouk E.A., Philatov G.P. / Беззатеев С.В., ЛитВИНОВ М.Ю., Крук Е.А., Филатов Г.П. / Converted Transformation of the Image with the Structure Destroying // XI International Symposium on Problems of Redundancy in Information and Control Systems: Proceeding/ Saint-Petersburg State University of Aerospace Instrumentation (SUAI), 2007.
106. Litvinov M.Y., Sergeev M.B., Sergeev A.M. (ЛитВИНОВ М. Ю.,Сергеев М. Б., Сергеев А. М.) Problems on Formation Protected Digital Images // XI International Symposium on Problems of Redundancy in Information and Control Systems: Proceeding/ Saint-Petersburg State University of Aerospace Instrumentation (SUAI), 2007.

Оглавление

Стр.

Глава IV. Раскрытие преступлений, совершаемых в системе дистанционного банковского обслуживания	3
4.1. Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых в системе дистанционного банковского обслуживания	7
4.2. Некоторые способы хищения денежных средств в системе дистанционного банковского обслуживания	20
4.3. Особенности раскрытия преступлений, связанных с хищением денежных средств в системе дистанционного банковского обслуживания	46
4.4. Особенности производства отдельных следственных действий на начальном этапе расследования преступлений, совершаемых в системе дистанционного банковского обслуживания	63
4.5. Профилактика хищений денежных средств в системе дистанционного банковского обслуживания	75
Глава V. Обзор преступлений, совершенных в условиях цифровизации	78
Глава VI. Противодействие перехвату оперативно значимой информации преступными элементами способом маскирования	92
6.1. Алгоритмы маскирующих преобразований видеоинформации	92
6.2. Форматы данных. Избыточность и сжатие	93
6.2.1. <i>BMP</i>	93
6.2.2. <i>JPEG</i>	93
6.2.3. <i>Motion JPEG</i>	94
6.2.4. <i>MPEG</i>	95
6.2.5. Особенности функционирования систем видеоконтроля	95
6.2.6. Особенности маскирования видеопотока и изображений	96
6.2.7. Соккрытие первичной информации	96
6.2.8. Соккрытие вторичной информации	98
6.3. Обзор существующих методов маскирования	99
6.3.1. Классификация методов	99
6.3.1.1. Сплошное маскирование	100
6.3.1.2. Методы с выборочным маскированием	101
6.3.2. Алгоритмы симметричного шифрования	104
6.3.2.1. Алгоритм ГОСТ 28147-89	104
6.3.2.2. Сравнение режимов шифрования	105
6.3.2.3. Программная реализация ГОСТ	107
6.3.2.4. ГОСТ с редуцированным числом раундов	107

6.4. Выбор маскирующего преобразования	108
6.4.1. Структура системы видеоконтроля с защищенной передачей	108
6.4.2. Схемы и режимы маскирования	109
6.4.3. Маскирование потока бит видеоинформации	109
6.4.4. Маскирование половины потока бит видеоинформации	110
6.4.5. Параллельное маскирование разделенного потока бит видеоинформации	111
6.4.6. Использование схем облегченного маскирования	111
6.4.7. Защита данных в формате BMP	112
6.4.8. Особенности кодирования Хаффмана в JPEG и маскирование	112
6.4.8.1. Структура данных, обрабатываемых кодером JPEG	113
6.4.8.2. Энтропийное кодирование	114
6.4.8.3. Кодирование DC коэффициентов	114
6.4.8.4. Кодирование AC коэффициентов	116
6.4.8.5. Однотонные полосы при маскировании	116
6.4.8.6. Неполное отображение кадра	117
6.4.9. Уничтожение первичной информации	117
6.4.9.1. Общие принципы сокрытия первичной информации в JPEG	117
6.4.9.2. Формирование и передача ключевой информации	117
6.4.9.3. Правила генерации ключей и синхропосылки	118
6.4.10. Уничтожение вторичной информации	119
6.4.10.1. Вычисление эффективной длины кадра	120
6.4.11. Возможные методы анализа вторичной информации	133
6.4.11.1. Анализ без использования какой-либо дополнительной информации	133
6.4.11.2. Анализ при использовании пар исходного и маскированного изображения	135
6.4.11.3. Анализ по выбранному исходному изображению	136

Глава VII.

Маскирование, основанное

на методах теории помехоустойчивого кодирования

7.1. Система МакЭлиса несимметричного шифрования, использующая коды, исправляющие ошибки	138
---	-----

7.2. Модификация схемы МакЭлиса для шифрации видеоизображения	140
--	-----

7.3. Пример использования модифицированной схемы МакЭлиса	144
--	-----

Заключение	145
-------------------------	------------

Литература	150
-------------------------	------------

Научное издание

Литвинов Михаил Юрьевич,
кандидат технических наук
Алескеров Вагиф Исмаилович,
кандидат юридических наук, доцент

**ПРОТИВОДЕЙСТВИЕ
СОВРЕМЕННЫМ ВИДАМ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

Часть 2

Редактирование О.Н. Колокольчикова
Техническое редактирование Е.В. Бухарина

Подписано в печать 30.06.2026.
Формат 60х84 1/16. Объем 10,0 усл.-изд. л.
Тираж 100 экз. Заказ 09/26. Цена договорная.

Федеральное государственное казенное учреждение
дополнительного профессионального образования
«Всероссийский институт повышения квалификации сотрудников

Министерства внутренних дел Российской Федерации».
142007, Московская обл., г. Домодедово, микрорайон Авиационный,
ул. Пихтовая, д. 3.