Секция «Проблемы финансовых расследований и экономической безопасности»

Типовые схемы легализации преступных доходов, полученных в результате совершения киберпреступлений в кредитно-финансовой системе

Научный руководитель – Сомик Кирилл Васильевич

Насибов Мехтихан Зиятхан оглы

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия

E-mail: metikmetik@gmail.com

В последние годы наблюдается значительный рост киберпреступлений в кредитно-финансовой сфере, которые не только наносят масштабный экономический ущерб, но и путем легализации получаемых преступных доходов продуцируют криминализацию финансовой системы. Так, по данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) в 2017 году в результате кибератак на банки было похищено более миллиарда рублей. В отношении физических лиц в результате несанкционированных транзакций с использованием банковских карт в 2017 году было похищено около миллиарда рублей. Серьезные проблемы имеют место и у корпоративных клиентов банков. Объем хищений денежных средств со счетов юридических лиц с использованием систем дистанционного банковского обслуживания (ДБО) в 2017 году составил 1,57 миллиарда рублей [8].

Анализ показывает, что наибольшую опасность в современных условиях представляют киберпреступления, квалифицируемые Уголовным кодексом Российской Федерации как мошенничество с использованием электронных средств платежа (ст.159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст.159.6 УК РФ). Именно эти преступления являются предикатными и формируют незаконные доходы в значительных масштабах. Вместе с тем, необходимо отметить, что еще большую потенциальную опасность представляют преступления, квалифицируемые как неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Хотя формально такие преступления не являются корыстными и напрямую не продуцируют преступные доходы для последующего отмывания, но они представляют самую большую опасность для экономики и финансовой системы. Дело в том, что через информационные системы и телекоммуникационные сети национальной платежной системы (НПС) ежегодно проходят гигантские потоки денежных средств, объем которых измеряется тысячами триллионов рублей. В этой связи необходимо иметь ввиду, что результативная системная кибератака в отношении такой структуры может привести к коллапсу всей финансовой системы. Однако, здесь нужно отметить, что согласно экспертным оценкам современная высокотехнологичная инфраструктура НПС отвечает повышенным требованиям обеспечения экономической, финансовой и информационной безопасности.

В связи с вышеизложенным на основе анализа судебной практики была разработана типовая схема легализации преступных доходов, полученных в результате мошенничества в сфере компьютерной информации (рис.1). Данная схема является результатом обобщения типичных действий, выявленных и доказанных в ходе расследования и рассмотрения в суде нескольких аналогичных дел по статье 159.6 и последующей легализации полученных преступных доходов, квалифицированных по статье 174.1. Предикатное преступление в данной схеме представляет мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование средств хранения,

обработки компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба и совершенное лицом с использованием своего служебного положения.

Анализ рассмотренной схемы показал наличие серьезных проблем, прежде всего, в части своевременного выявления и документирования киберпреступлений в форме мошенничества в сфере компьютерной информации, а также использования электронных средств платежей. Необходимым условием решения этих проблем является разработка согласованных с Министерством юстиции Российской Федерации инструкции о порядке раскрытия операторами сотовой связи и интернет - провайдерами информации в отношении физических и юридических лиц, осуществляющих финансовые операции и иные действия, дающие основания подозревать их в подготовке и совершении киберпреступлений с целью последующей легализации получаемых преступных доходов.

Целесообразно также усовершенствовать правовые основы противодействия рассматриваемым видам преступлений в части: уточнения правового статуса электронных документов и иных электронных данных в целях признания их равнозначными оригиналам документов и сведениям на бумажных носителях в качестве доказательств при расследовании киберпреступлений и в уголовном процессе; регламентации механизмов международного взаимодействия центральных банков и правоохранительных органов разных стран при противодействии киберпреступлениям трансграничного характера; установления ограничений, направленных на снижение количества анонимных способов осуществления операций с использованием платежных услуг, в том числе, с применением электронных средств платежа; использования многофакторной/мультиканальной аутентификации.

В последние годы наблюдается значительный рост киберпреступлений в кредитно-финансовой сфере, которые не только наносят масштабный экономический ущерб, но и путем легализации получаемых преступных доходов продуцируют криминализацию финансовой системы. Так, по данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) в 2017 году в результате кибератак на банки было похищено более миллиарда рублей. В отношении физических лиц в результате несанкционированных транзакций с использованием банковских карт в 2017 году было похищено около миллиарда рублей. Серьезные проблемы имеют место и у корпоративных клиентов банков. Объем хищений денежных средств со счетов юридических лиц с использованием систем дистанционного банковского обслуживания (ДБО) в 2017 году составил 1,57 миллиарда рублей [6].

Анализ показывает, что наибольшую опасность в современных условиях представляют киберпреступления, квалифицируемые Уголовным кодексом Российской Федерации как мошенничество с использованием электронных средств платежа (ст.159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст.159.6 УК РФ). Именно эти преступления являются предикатными и формируют незаконные доходы в значительных масштабах. Вместе с тем, необходимо отметить, что еще большую потенциальную опасность представляют преступления, квалифицируемые как неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Хотя формально такие преступления не являются корыстными и напрямую не продуцируют преступные доходы для последующего отмывания, но они представляют самую большую опасность для экономики и финансовой системы. Дело в том, что через информационные системы и телекоммуникационные сети национальной платежной системы (НПС) ежегодно проходят гигантские потоки денежных средств, объем которых измеряется тысячами триллионов рублей. В этой связи необходимо иметь ввиду, что результативная системная кибератака в отношении такой структуры может привести к коллапсу всей финансовой

системы. Однако, здесь нужно отметить, что согласно экспертным оценкам современная высокотехнологичная инфраструктура НПС отвечает повышенным требованиям обеспечения экономической, финансовой и информационной безопасности.

В связи с вышеизложенным на основе анализа судебной практики была разработана типовая схема легализации преступных доходов, полученных в результате мошенничества в сфере компьютерной информации (рис.1). Данная схема является результатом обобщения типичных действий, выявленных и доказанных в ходе расследования и рассмотрения в суде нескольких аналогичных дел по статье 159.6 и последующей легализации полученных преступных доходов, квалифицированных по статье 174.1. Предикатное преступление в данной схеме представляет мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование средств хранения, обработки компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба и совершенное лицом с использованием своего служебного положения.

Анализ рассмотренной схемы показал наличие серьезных проблем, прежде всего, в части своевременного выявления и документирования киберпреступлений в форме мошенничества в сфере компьютерной информации, а также использования электронных средств платежей. Необходимым условием решения этих проблем является разработка согласованных с Министерством юстиции Российской Федерации инструкции о порядке раскрытия операторами сотовой связи и интернет - провайдерами информации в отношении физических и юридических лиц, осуществляющих финансовые операции и иные действия, дающие основания подозревать их в подготовке и совершении киберпреступлений с целью последующей легализации получаемых преступных доходов.

Целесообразно также усовершенствовать правовые основы противодействия рассматриваемым видам преступлений в части: уточнения правового статуса электронных документов и иных электронных данных в целях признания их равнозначными оригиналам документов и сведениям на бумажных носителях в качестве доказательств при расследовании киберпреступлений и в уголовном процессе; регламентации механизмов международного взаимодействия центральных банков и правоохранительных органов разных стран при противодействии киберпреступлениям трансграничного характера; установления ограничений, направленных на снижение количества анонимных способов осуществления операций с использованием платежных услуг, в том числе, с применением электронных средств платежа; использования многофакторной/мультиканальной аутентификации.

В последние годы наблюдается значительный рост киберпреступлений в кредитно-финансовой сфере, которые не только наносят масштабный экономический ущерб, но и путем легализации получаемых преступных доходов продуцируют криминализацию финансовой системы. Так, по данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) в 2017 году в результате кибератак на банки было похищено более миллиарда рублей. В отношении физических лиц в результате несанкционированных транзакций с использованием банковских карт в 2017 году было похищено около миллиарда рублей. Серьезные проблемы имеют место и у корпоративных клиентов банков. Объем хищений денежных средств со счетов юридических лиц с использованием систем дистанционного банковского обслуживания (ДБО) в 2017 году составил 1,57 миллиарда рублей [6].

Анализ показывает, что наибольшую опасность в современных условиях представляют киберпреступления, квалифицируемые Уголовным кодексом Российской Федерации как мошенничество с использованием электронных средств платежа (ст.159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст.159.6 УК РФ). Именно эти пре-

ступления являются предикатными и формируют незаконные доходы в значительных масштабах. Вместе с тем, необходимо отметить, что еще большую потенциальную опасность представляют преступления, квалифицируемые как неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Хотя формально такие преступления не являются корыстными и напрямую не продуцируют преступные доходы для последующего отмывания, но они представляют самую большую опасность для экономики и финансовой системы. Дело в том, что через информационные системы и телекоммуникационные сети национальной платежной системы (НПС) ежегодно проходят гигантские потоки денежных средств, объем которых измеряется тысячами триллионов рублей. В этой связи необходимо иметь ввиду, что результативная системная кибератака в отношении такой структуры может привести к коллапсу всей финансовой системы. Однако, здесь нужно отметить, что согласно экспертным оценкам современная высокотехнологичная инфраструктура НПС отвечает повышенным требованиям обеспечения экономической, финансовой и информационной безопасности.

В связи с вышеизложенным на основе анализа судебной практики была разработана типовая схема легализации преступных доходов, полученных в результате мошенничества в сфере компьютерной информации (рис.1). Данная схема является результатом обобщения типичных действий, выявленных и доказанных в ходе расследования и рассмотрения в суде нескольких аналогичных дел по статье 159.6 и последующей легализации полученных преступных доходов, квалифицированных по статье 174.1. Предикатное преступление в данной схеме представляет мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование средств хранения, обработки компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба и совершенное лицом с использованием своего служебного положения.

Анализ рассмотренной схемы показал наличие серьезных проблем, прежде всего, в части своевременного выявления и документирования киберпреступлений в форме мошенничества в сфере компьютерной информации, а также использования электронных средств платежей. Необходимым условием решения этих проблем является разработка согласованных с Министерством юстиции Российской Федерации инструкции о порядке раскрытия операторами сотовой связи и интернет - провайдерами информации в отношении физических и юридических лиц, осуществляющих финансовые операции и иные действия, дающие основания подозревать их в подготовке и совершении киберпреступлений с целью последующей легализации получаемых преступных доходов.

Целесообразно также усовершенствовать правовые основы противодействия рассматриваемым видам преступлений в части: уточнения правового статуса электронных документов и иных электронных данных в целях признания их равнозначными оригиналам документов и сведениям на бумажных носителях в качестве доказательств при расследовании киберпреступлений и в уголовном процессе; регламентации механизмов международного взаимодействия центральных банков и правоохранительных органов разных стран при противодействии киберпреступлениям трансграничного характера; установления ограничений, направленных на снижение количества анонимных способов осуществления операций с использованием платежных услуг, в том числе, с применением электронных средств платежа; использования многофакторной/мультиканальной аутентификации.

В последние годы наблюдается значительный рост киберпреступлений в кредитно-финансовой сфере, которые не только наносят масштабный экономический ущерб, но и путем легализации получаемых преступных доходов продуцируют криминализацию финансовой системы. Так, по данным Центра мониторинга и реагирования на компьютерные атаки в

кредитно-финансовой сфере (ФинЦЕРТ Банка России) в 2017 году в результате кибератак на банки было похищено более миллиарда рублей. В отношении физических лиц в результате несанкционированных транзакций с использованием банковских карт в 2017 году было похищено около миллиарда рублей. Серьезные проблемы имеют место и у корпоративных клиентов банков. Объем хищений денежных средств со счетов юридических лиц с использованием систем дистанционного банковского обслуживания (ДБО) в 2017 году составил 1,57 миллиарда рублей [6].

Анализ показывает, что наибольшую опасность в современных условиях представляют киберпреступления, квалифицируемые Уголовным кодексом Российской Федерации как мошенничество с использованием электронных средств платежа (ст.159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст.159.6 УК РФ). Именно эти преступления являются предикатными и формируют незаконные доходы в значительных масштабах. Вместе с тем, необходимо отметить, что еще большую потенциальную опасность представляют преступления, квалифицируемые как неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Хотя формально такие преступления не являются корыстными и напрямую не продуцируют преступные доходы для последующего отмывания, но они представляют самую большую опасность для экономики и финансовой системы. Дело в том, что через информационные системы и телекоммуникационные сети национальной платежной системы (НПС) ежегодно проходят гигантские потоки денежных средств, объем которых измеряется тысячами триллионов рублей. В этой связи необходимо иметь ввиду, что результативная системная кибератака в отношении такой структуры может привести к коллапсу всей финансовой системы. Однако, здесь нужно отметить, что согласно экспертным оценкам современная высокотехнологичная инфраструктура НПС отвечает повышенным требованиям обеспечения экономической, финансовой и информационной безопасности.

В связи с вышеизложенным на основе анализа судебной практики была разработана типовая схема легализации преступных доходов, полученных в результате мошенничества в сфере компьютерной информации (рис.1). Данная схема является результатом обобщения типичных действий, выявленных и доказанных в ходе расследования и рассмотрения в суде нескольких аналогичных дел по статье 159.6 и последующей легализации полученных преступных доходов, квалифицированных по статье 174.1. Предикатное преступление в данной схеме представляет мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование средств хранения, обработки компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба и совершенное лицом с использованием своего служебного положения.

Анализ рассмотренной схемы показал наличие серьезных проблем, прежде всего, в части своевременного выявления и документирования киберпреступлений в форме мошенничества в сфере компьютерной информации, а также использования электронных средств платежей. Необходимым условием решения этих проблем является разработка согласованных с Министерством юстиции Российской Федерации инструкции о порядке раскрытия операторами сотовой связи и интернет - провайдерами информации в отношении физических и юридических лиц, осуществляющих финансовые операции и иные действия, дающие основания подозревать их в подготовке и совершении киберпреступлений с целью последующей легализации получаемых преступных доходов.

Целесообразно также усовершенствовать правовые основы противодействия рассматриваемым видам преступлений в части: уточнения правового статуса электронных документов и иных электронных данных в целях признания их равнозначными оригиналам документов и сведениям на бумажных носителях в качестве доказательств при рассле-

довании киберпреступлений и в уголовном процессе; регламентации механизмов международного взаимодействия центральных банков и правоохранительных органов разных стран при противодействии киберпреступлениям трансграничного характера; установления ограничений, направленных на снижение количества анонимных способов осуществления операций с использованием платежных услуг, в том числе, с применением электронных средств платежа; использования многофакторной/мультиканальной аутентификации.

В последние годы наблюдается значительный рост киберпреступлений в кредитно-финансовой сфере, которые не только наносят масштабный экономический ущерб, но и путем легализации получаемых преступных доходов продуцируют криминализацию финансовой системы. Так, по данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) в 2017 году в результате кибератак на банки было похищено более миллиарда рублей. В отношении физических лиц в результате несанкционированных транзакций с использованием банковских карт в 2017 году было похищено около миллиарда рублей. Серьезные проблемы имеют место и у корпоративных клиентов банков. Объем хищений денежных средств со счетов юридических лиц с использованием систем дистанционного банковского обслуживания (ДБО) в 2017 году составил 1,57 миллиарда рублей [6].

Анализ показывает, что наибольшую опасность в современных условиях представляют киберпреступления, квалифицируемые Уголовным кодексом Российской Федерации как мошенничество с использованием электронных средств платежа (ст.159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст.159.6 УК РФ). Именно эти преступления являются предикатными и формируют незаконные доходы в значительных масштабах. Вместе с тем, необходимо отметить, что еще большую потенциальную опасность представляют преступления, квалифицируемые как неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Хотя формально такие преступления не являются корыстными и напрямую не продуцируют преступные доходы для последующего отмывания, но они представляют самую большую опасность для экономики и финансовой системы. Дело в том, что через информационные системы и телекоммуникационные сети национальной платежной системы (НПС) ежегодно проходят гигантские потоки денежных средств, объем которых измеряется тысячами триллионов рублей. В этой связи необходимо иметь ввиду, что результативная системная кибератака в отношении такой структуры может привести к коллапсу всей финансовой системы. Однако, здесь нужно отметить, что согласно экспертным оценкам современная высокотехнологичная инфраструктура НПС отвечает повышенным требованиям обеспечения экономической, финансовой и информационной безопасности.

В связи с вышеизложенным на основе анализа судебной практики была разработана типовая схема легализации преступных доходов, полученных в результате мошенничества в сфере компьютерной информации (рис.1). Данная схема является результатом обобщения типичных действий, выявленных и доказанных в ходе расследования и рассмотрения в суде нескольких аналогичных дел по статье 159.6 и последующей легализации полученных преступных доходов, квалифицированных по статье 174.1. Предикатное преступление в данной схеме представляет мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование средств хранения, обработки компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба и совершенное лицом с использованием своего служебного положения.

Анализ рассмотренной схемы показал наличие серьезных проблем, прежде всего, в части своевременного выявления и документирования киберпреступлений в форме мо-

шенничества в сфере компьютерной информации, а также использования электронных средств платежей. Необходимым условием решения этих проблем является разработка согласованных с Министерством юстиции Российской Федерации инструкции о порядке раскрытия операторами сотовой связи и интернет - провайдерами информации в отношении физических и юридических лиц, осуществляющих финансовые операции и иные действия, дающие основания подозревать их в подготовке и совершении киберпреступлений с целью последующей легализации получаемых преступных доходов.

Целесообразно также усовершенствовать правовые основы противодействия рассматриваемым видам преступлений в части: уточнения правового статуса электронных документов и иных электронных данных в целях признания их равнозначными оригиналам документов и сведениям на бумажных носителях в качестве доказательств при расследовании киберпреступлений и в уголовном процессе; регламентации механизмов международного взаимодействия центральных банков и правоохранительных органов разных стран при противодействии киберпреступлениям трансграничного характера; установления ограничений, направленных на снижение количества анонимных способов осуществления операций с использованием платежных услуг, в том числе, с применением электронных средств платежа; использования многофакторной/мультиканальной аутентификации.

В последние годы наблюдается значительный рост киберпреступлений в кредитно-финансовой сфере, которые не только наносят масштабный экономический ущерб, но и путем легализации получаемых преступных доходов продуцируют криминализацию финансовой системы. Так, по данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) в 2017 году в результате кибератак на банки было похищено более миллиарда рублей. В отношении физических лиц в результате несанкционированных транзакций с использованием банковских карт в 2017 году было похищено около миллиарда рублей. Серьезные проблемы имеют место и у корпоративных клиентов банков. Объем хищений денежных средств со счетов юридических лиц с использованием систем дистанционного банковского обслуживания (ДБО) в 2017 году составил 1,57 миллиарда рублей [6].

Анализ показывает, что наибольшую опасность в современных условиях представляют киберпреступления, квалифицируемые Уголовным кодексом Российской Федерации как мошенничество с использованием электронных средств платежа (ст.159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст.159.6 УК РФ). Именно эти преступления являются предикатными и формируют незаконные доходы в значительных масштабах. Вместе с тем, необходимо отметить, что еще большую потенциальную опасность представляют преступления, квалифицируемые как неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Хотя формально такие преступления не являются корыстными и напрямую не продуцируют преступные доходы для последующего отмывания, но они представляют самую большую опасность для экономики и финансовой системы. Дело в том, что через информационные системы и телекоммуникационные сети национальной платежной системы (НПС) ежегодно проходят гигантские потоки денежных средств, объем которых измеряется тысячами триллионов рублей. В этой связи необходимо иметь ввиду, что результативная системная кибератака в отношении такой структуры может привести к коллапсу всей финансовой системы. Однако, здесь нужно отметить, что согласно экспертным оценкам современная высокотехнологичная инфраструктура НПС отвечает повышенным требованиям обеспечения экономической, финансовой и информационной безопасности.

В связи с вышеизложенным на основе анализа судебной практики была разработана типовая схема легализации преступных доходов, полученных в результате мошенничества

в сфере компьютерной информации (рис.1). Данная схема является результатом обобщения типичных действий, выявленных и доказанных в ходе расследования и рассмотрения в суде нескольких аналогичных дел по статье 159.6 и последующей легализации полученных преступных доходов, квалифицированных по статье 174.1. Предикатное преступление в данной схеме представляет мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование средств хранения, обработки компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба и совершенное лицом с использованием своего служебного положения.

Анализ рассмотренной схемы показал наличие серьезных проблем, прежде всего, в части своевременного выявления и документирования киберпреступлений в форме мошенничества в сфере компьютерной информации, а также использования электронных средств платежей. Необходимым условием решения этих проблем является разработка согласованных с Министерством юстиции Российской Федерации инструкции о порядке раскрытия операторами сотовой связи и интернет - провайдерами информации в отношении физических и юридических лиц, осуществляющих финансовые операции и иные действия, дающие основания подозревать их в подготовке и совершении киберпреступлений с целью последующей легализации получаемых преступных доходов.

Целесообразно также усовершенствовать правовые основы противодействия рассматриваемым видам преступлений в части: уточнения правового статуса электронных документов и иных электронных данных в целях признания их равнозначными оригиналам документов и сведениям на бумажных носителях в качестве доказательств при расследовании киберпреступлений и в уголовном процессе; регламентации механизмов международного взаимодействия центральных банков и правоохранительных органов разных стран при противодействии киберпреступлениям трансграничного характера; установления ограничений, направленных на снижение количества анонимных способов осуществления операций с использованием платежных услуг, в том числе, с применением электронных средств платежа; использования многофакторной/мультиканальной аутентификации.

Источники и литература

1) Зубков В.А., Осипов С.К. Международные стандарты в сфере противодействия отмыванию преступных доходов и финансированию терроризму: Учебное пособие. — М.: Юриспруденция, 2012
2) Пикуров Н.И. Налоговые преступления как предикатные в отношении легализации преступных доходов: подходы к реализации международных стандартов. Международный учебно-методический центр финансового мониторинга. 2014.
3) Ревенков П.В., Липатов А.О., Платежные услуги с использованием электронных средств платежа и противодействие легализации (отмыванию) доходов, полученных преступным путем. М.: Журнал «Деньги и кредит». №12, 2017 г.
4) Стратегия обеспечения экономической безопасности до 2030 года.
5) Федеральный закон «О противодействии легализации доходов, полученных преступным путем» №115 - ФЗ.
6) Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» №187 –ФЗ.
7) Отчет генеральной прокуратуры. genproc.gov.ru, 2017 г.
8) Отчет ФинЦЕРТ Банка России за 2017-2018 г.г. www.cbr.ru

Иллюстрации

Рис. 1. Типовая схема легализации доходов, полученных в результате киберпреступлений в кредитно-финансовой системе