

Государственное бюджетное профессиональное образовательное учреждение
«Арзамасский коммерческо-технический техникум»

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ
РАБОТ**

ОП 13 «Безопасность банковской деятельности»

Специальность 38.02.07 Банковское дело

Одобрена методическим
объединением экономических
дисциплин

Протокол № ____

от « ____ » _____ 20 ____ г

Председатель МО:

Составлены в соответствии с
требованиями к результатам
освоения ППССЗ (ППКРС) по
специальности 38.02.07 Банковское
дело Зам. директора по УПРиЭД

Автор:

Т.И.Гордеева, преподаватель специальных дисциплин первой квалификационной категории ГБПОУ «Арзамасский коммерческо-технический техникум»

Методические указания содержат задания к практическим работам, порядок их выполнения, рекомендации, перечень контрольных вопросов по каждой практической работе, требования к знаниям и умениям. Приведен список основной литературы и нормативных документов, рекомендуемых для подготовки к практическим работам.

Методические указания предназначены для студентов специальности **38.02.07** «Банковское дело».

СОДЕРЖАНИЕ

Введение	4
Практическая работа № 1 "Причины совершения и характеристика наиболее характерных преступлений в банковской сфере"	6
Практическая работа № 2 "Анализ защищенности конфиденциальной банковской информации"	9
Практическая работа № 3 "Проблемы безопасности электронных платежей и банковских платежных карт"	13
Практическая работа № 4 "Действия службы безопасности и сотрудников банка в кризисных ситуациях"	18
	20
Практическая работа № 5 «Противодействие легализации(отмыванию)доходов, полученных преступным путем, и финансирование терроризма».	
Практическая работа № 6 "Использование технических средств в целях защиты банковской тайны"	27

Введение

Практические работы направлены на формирование практических умений необходимых при освоении учебной дисциплины :

- профессиональных (выполнять определенные действия, операции, предписания, необходимые в последующем в профессиональной деятельности);
- учебных .

В процессе практического занятия студенты выполняют одну или несколько практических работ (заданий) под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.

Содержанием практических работ является решение различного рода задач, в том числе профессиональных (анализ производственных задач и т. п.), работа с нормативными документами, инструктивными материалами, справочниками и др.

Состав заданий для практического занятия спланирован с расчетом, чтобы за отведенное время они могли быть выполнены качественно большинством студентов.

Выполнению практических работ предшествует проверка знаний студентов – их теоретической готовности к выполнению задания.

Формы организации работы студентов на практических работах могут быть: фронтальная, групповая и индивидуальная.

При фронтальной форме организации работ все студенты выполняют одновременно одну и ту же работу.

При групповой форме организации работ одна и та же работа выполняется микрогруппами по 2-5 человек.

При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.

Выполнение практических работ по учебной дисциплине ОП.13 «Безопасность банковской деятельности» направлено на *формирование общих компетенций*

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.

ОК 11. Знать правила техники безопасности, нести ответственность за организацию мероприятий по обеспечению безопасности труда.

Выполнение практических работ по дисциплине ОП13 «Безопасность банковской деятельности» ***направлено на формирование профессиональных компетенций***

ПК 1.6. Обслуживать расчетные операции с использованием различных видов платежных карт

ПК 2.1. Оценивать кредитоспособность клиентов.

ПК 2.2. Осуществлять и оформлять выдачу кредитов

Практическая работа1 Причины совершения и характеристика наиболее характерных преступлений в банковской сфере России

ЦЕЛЬ РАБОТЫ: формирование практических умений и навыков по классификации и характеристике преступлений в банковской сфере России

Для выполнения работы необходимо **знать** организационные основы банковской деятельности, функции подразделений безопасности банков, вопросы соблюдения прав и свобод личности при решении задач обеспечения безопасности; необходимо **уметь** выявить попытки финансирования преступлений; оценивать степень угрозы личной безопасности банковского специалиста;

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Классификация преступлений в кредитно-банковской сфере может быть осуществлена по различным основаниям в зависимости от целей изучения явления.

Преступления в банковской сфере условно можно разделить на две группы:

1 - насильственные преступления (убийства, налеты, грабежи и т.д.);

2 - «беловоротничковые» преступления (финансовые хищения и махинации).

Вторая группа преобладает как количественно, так и по объемам похищенных средств.

1- Насильственные преступления

1.1 Покушения на руководителей и персонал банков.

Наибольшую угрозу для банка представляют покушения на руководящих сотрудников банка.

Наиболее распространенным видом преступлений против банкиров являются заказные убийства.

1.2 Похищения, вымогательства, кражи.

Рэкет, вымогательства, кражи имеют очень низкую раскрываемость.

1.3 Ограбления и налеты на банки.

Наиболее часто объектом налета становятся не центральные офисы банков, а их филиалы, отделения и валютные обменные пункты, уровень безопасности которых ниже или вообще находится на несоответствующем профилю учреждения уровне.

2-Финансовые преступления

2.1 Махинации с государственными и бюджетными средствами.

Распространенное явление - это нерациональное и нецелевое использование государственных кредитных ресурсов и бюджетных средств. При непосредственном участии работников банковской сферы идет перекачка государственных денег в частные структуры.

2.2 Мошенничества с деньгами вкладчиков

Дела об обманутых вкладчиках стали важной социальной проблемой в России. Создано огромное количество финансовых и трастовых компаний, активно рекламировавших свою деятельность, а затем исчезавших бесследно.

2.3 Невозвращение средств в иностранной валюте из-за рубежа

Серьезным преступлением является невозврат или неполное возвращение валютной выручки, полученной от экспортных операций. Используются лжеэкспортные поставки, участниками которых являются работники ликероводочных и автомобильных заводов, таможен и банков.

2.4 Лжекредитование

Лжекредитование, то есть присвоение кредитов по фиктивным банковским гарантиям подставными фирмами. Сразу после получения кредита такие фирмы прекращают свое существование.

2.5 Подложные гарантийные документы

Например, фирма, используя подложные гарантийные документы Центрального банка, похищает деньги в коммерческом банке.

2.6 Мошенничество с кредитом под залог

Возможно получение кредитов под многократно заложенное имущество, под имущество, не зарегистрированное, под уже не принадлежащее данному лицу имущество и т.п. Возможны также вероятность предоставления фиктивного баланса предприятия и ложных сведений о имущественном и материальном состоянии, фиктивности самого коммерческого предприятия, предоставление поддельных гарантий.

2.7 Хищение кредитов фирмами, зарегистрированными по подложным документам.

2.8 Взаимное кредитование банков по сговору.

2.9 Хищение средств, незаконно используя генеральную доверенность Сбербанка

2.10 Многократное получение кредитов в разных банках

2.11 Хищение кредитов фирмами по поддельным договорам

2.12 Получение кредита под фальшивый контракт

2.13 Хищение денег по аккредитиву под поставку товаров

2.14 Попытка раскрытия аккредитива под поставку товаров

2.15 Мошенничество от имени авторитетных государственных структур, таких как Управление Центральным банком, Пенсионный Фонд и т.п.

2.16 Услуги по списанию средств из Фонда обязательных резервов

2.17 Поддельные приказы арбитражного суда

2.18 Обман банков с использованием поддельных удостоверений администрации Президента

2.19 Мошенничество от имени мэрии

2.20 Фальшивые авизо

2.21 Подложные мемориальные ордера

2.22 Мошенничества с применением компьютерной техники и телекоммуникаций. Некоторые направления развития компьютерных преступлений:

2.23 Махинации с чеками

2.24 Мошенничество с ценными бумагами

2.25 Международные финансовые преступления

2.26 Фальшивомонетничество и подделка государственных ценных бумаг

2.27 Мошенничества с пластиковыми карточками:

- незаконное использование подлинных кредиток, которые были утеряны их владельцем или украдены у него;
- использование частично переделанной карточки;
- изготовление и использование поддельных карт.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1 По материалам конспекта лекций по теме «Наиболее характерные преступления, совершаемые в банковской сфере» составьте кластер «Классификация преступлений в банковской сфере России»

Задание 2 Составьте таблицу «Насильственные преступления в отношении персонала и имущества банков»

Задание 3 Составьте таблицу «Финансовые преступления в банковской сфере»

Задание 4 Преступления в банковской сфере условно можно разделить на две группы:

1 - насильственные преступления (убийства, налеты, грабежи и т.д.);

2 - «беловоротничковые» преступления (финансовые хищения и махинации)

Какая из групп преобладает как количественно, так и по объемам похищенных средств. Почему вторая группа получила название «беловоротничковые преступления»

Задание 5 Определите вид преступления в банковской сфере кредитования

А Кузнецова А.В., получил кредит в банке «Восток Экспресс» в размере 80.000 рублей, предоставив в банк фиктивные документы на право получения указанных кредитных средств.

Б Предприимчивая гражданка И. создала и возглавила общество с ограниченной ответственностью. Уже через месяц после регистрации ООО получило от крупного ОАО беспроцентный кредит в виде векселей, выданных правительством субъекта РФ. Взамен ООО обязалось поставить в адрес ОАО шерсть и автомобили. Векселя были предъявлены к оплате. После зачисления денег на счет ООО гражданка И. купила автомобили себе и своим родственникам, приобрела роскошную мебель, несколько раз съездила за рубеж, оформив эти поездки как служебные командировки и т. д. Конечно, обещанных товаров ОАО так и не дождалось ни через полгода, ни через год... После того как ООО и его учредителем заинтересовался ОБЭП, по инициативе правоохранительных органов в ООО была проведена ревизия. По ее результатам выяснилось, что деятельность этой коммерческой организации с самого момента создания была убыточна. Гражданке И. было предъявлено обвинение, и она была осуждена по ст. 173 УК РФ

В Гражданин К. зарегистрировал хозяйственное общество, открыл счет в банке и получил в этом же банке кредит для закупки товаров народного потребления. Кредит не был возвращен в срок. Тогда банк, предварительно проведя собственное расследование, обратился в правоохранительные органы. Финансовая проверка, проведенная представителями уполномоченных органов, показала, что поступившие на счет организации-заемщика денежные средства были обналичены небольшими суммами, которые учредитель расходовал на личные нужды. Выяснилось и то, что за все время своего существования хозяйственное общество не вело никакой деятельности.

Задание 6 Составьте по теме «Характерные преступления в банковской сфере России» тест не менее 10 вопросов

Задание 7* По материалам сайтов Интернет подготовить доклад о совершенном преступлении в банковской сфере.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1 От чего зависит классификация преступлений в кредитно-банковской сфере?
- 2 На какие группы можно условно разделить преступления в банковской сфере ?
- 3 Какие преступления относятся к насильственным?
- 4 Какие преступления относятся к «беловоротничковым»?

Практическая работа № 2 Анализ защищенности конфиденциальной банковской информации

ЦЕЛЬ РАБОТЫ: формирование практических умений и навыков по проведению анализа защищенности конфиденциальной банковской информации.

Для выполнения работы необходимо **знать** правовые основы охраны коммерческой тайны и защиты конфиденциальной банковской информации; источники и угрозы утечки конфиденциальной информации в банке; необходимо **уметь** определять возможные источники утечки информации; применять необходимые методы и средства защиты банковской информации, соблюдать, правила информационной безопасности банковских систем;

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Конфиденциальная информация – это документированная(приватная) информация в электронном или бумажном виде, содержание которой доступно только определенной группе людей, а ее передача третьим лицам является грубым нарушением законодательства Российской Федерации.

Конфиденциальная информация – это коммерческая, военная, банковская, служебная или государственная тайна. Как правило, конфиденциальная информация может представлять собой особую категорию и относиться к коммерческой тайне.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

Обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

Передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

Предоставление информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

Разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится

известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию обязаны предоставить эту информацию :

- Федеральной службы по финансовому мониторингу в ходе борьбы с нелегально полученными доходами.
- Следственных органов на этапе расследования преступлений.
- Службы судебных приставов на этапе изъятия имущества для погашения долговых обязательств.
- Центрального банка в ходе сбора статистической и аналитической информации.
- Судов различной инстанции.
- Налоговой инспекции в случае рассмотрения дел об уклонении от уплаты налогов.
- Агентства по страхованию вкладов .

Правовое понятие банковской тайны обычно подразумевает весь массив данных, который клиент добровольно предает в распоряжение финансового учреждения для получения конкретных услуг.

Банковская тайна включает:

1. Реквизиты юридических лиц.
2. Паспортные и контактные данные физических лиц.
3. Данные касательно уровня располагаемого клиентом дохода.
4. Финансовые реквизиты банковских карт и всевозможных типов расчетных счетов.
5. Информацию об имущественных правах, включая залоговое и полученное в кредит имущество.
6. Данные об открытии или закрытии счетов (номер, валюта, тип, срок действия и дата подписания соглашения).
7. Финансовые сводки о выполненных транзакциях, движении денежных средств и общем объеме операций.

Основной перечень сведений, которые официально составляют банковскую тайну, требуется финансовым учреждениям для ведения операционной деятельности и составления общего бухгалтерского баланса предприятия. Предоставляемая личная или корпоративная информация может разглашаться только после согласования с клиентом условий рассекречивания отдельных данных. За умышленную передачу секретной информации третьим лицам в целях получения выгоды предусмотрено уголовное наказание. Государственные органы получают доступ к конфиденциальным данным без согласия клиента и банка в рамках процедуры сбора информации для формирования аналитических отчетов, проведения проверок и расследования преступлений.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1

Определите ,что из перечисленного вы отнесли бы к сведениям, составляющим коммерческую тайну, банковскую тайну, а какие сведения не относятся к конфиденциальной банковской информации. Ответ оформите в таблице.

1. схемы и чертежи здания кредитной организации,
2. Банковские сделки,
3. Паспортные данные клиентов банка (для физических лиц);
4. учредительная документация и Устав банка
5. данные об уровне заработной платы сотрудников банка;
6. персональные данные сотрудников;
7. наличии свободных рабочих мест в компании;
8. документация, подтверждающая уплату налогов и обязательных платежей;
9. режим работы банка
10. управленческие решения
11. Тарифы на банковские услуги

12. Факт открытия счета (счетов), его номер и дата открытия, тип счета, валюта счета;
13. протоколы совещаний;
14. Курсы покупки и продажи валюты
15. сведения о кадровом составе, штатном расписании;
16. Реквизиты банка
17. Факт открытия счета (счетов), его номер и дата открытия, тип счета, валюта счета;
18. Факт наличия средств на счету (деньги, обезличенные металлические счета), сумма, проценты по вкладу, срок договора;
19. Номер лицензии.
20. процентная ставка по кредитам
21. Движение денежных средств на счетах и депозитных вкладах.
22. Процентная ставка по вкладам

Задание 2

Кому банк может сообщить сведения, составляющие банковскую тайну, о счетах граждан?

Ответ поясните.

- Суду;
- Росфинмониторингу;
- Служба судебных приставов;
- Родственникам
- Наследникам
- После смерти вкладчика лицам ,указанным в завещательном распоряжении на вклад
- Центральный банк Российской Федерации;
- Лицам, действующим на основании доверенности
- Агентству по страхованию вкладов;
- Органам предварительного следствия
- Владельцу счета по телефону.

Задание 3

Составьте таблицу отличия и сходства банковской и коммерческой тайны

Задание 4

Основным каналом утечки данных становятся, как правило, сотрудники. Перечислите причины утечки банковской информации через персонал банка. Какие меры эффективной системы защиты конфиденциальной информации от утечки через сотрудников банка могли бы вы предложить..

Задание 5

Иногда фирмы внедряют строгий контроль и учёт, организуют отдельный доступ персонала к тайне, подписывают соглашение по поводу защиты коммерческой тайны со всеми взаимодействующими предприятиями, но забывают обозначить сроки, во время которых данные являются конфиденциальными. Опишите последствия, к которым может привести данная ошибка.

Задание 6

Какие действия сотрудника банка ,указывают на попытку хищения конфиденциальной банковской информации?

1. Сотрудник работает сверхурочно.
2. Сотрудник банка беспричинно задерживается или регулярно начинает рабочий день значительно раньше положенного времени
3. Сотрудник банка в свободное время играет в компьютерные игры.
4. Без видимой необходимости служащий накапливает на своем компьютере и мобильных носителях большие объемы корпоративной информации.
5. Сотрудник много разговаривает по телефону.

6. Делает непредусмотренные копии внутренних документов, предназначенных только для служебного пользования.
7. Сотрудник недоволен начальством.
8. Нарушает внутрикорпоративные правила – использует несанкционированное программное обеспечение, собственную оргтехнику, посещает запрещённые сайты и публикует в Интернете информацию
9. Сотрудник замечен в связях с представителями конкурирующих компаний и их партнеров

КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1 Какую информацию следует считать конфиденциальной?
- 2 Какая информация составляет коммерческую тайну?
- 3 Кто является обладателем информации, составляющей коммерческую тайну?
- 4 Чем отличается передача информации от ее предоставления?
- 5 Какую информацию включает в себя банковская тайна ?
- 6 В чем отличие коммерческой тайны от банковской тайны?
- 7 Как вы думаете ,можно ли считать банковскую тайну разновидностью коммерческой тайны ?
- 8 Какие меры по охране конфиденциальности информации, составляющей коммерческую тайну, должны приниматься ее обладателем?

Практическая работа № 3 Проблемы безопасности электронных платежей и банковских платежных карт

ЦЕЛЬ РАБОТЫ формирование практических умений и навыков по проведению классификации и анализу проблемы безопасности электронных платежей и банковских платежных карт.

Для выполнения работы необходимо **знать** принципы защиты персональных платежей, в том числе с использованием электронных пластиковых карт, и обеспечения безопасности электронных межбанковских расчётов; необходимо **уметь** применять необходимые методы и средства защиты банковской информации, соблюдать, правила информационной безопасности банковских систем

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Способы хищения денежных средств в сфере обслуживания держателей банковских карт имеют специфические различия, которые определяются причастностью (либо непричастностью) к совершению преступления персонала банка.

В число основных способов хищения **персоналом банков** денежных средств в сфере обслуживания держателей банковских карт входят:

- оформление кредитных карт на имя неосведомленных об этом клиентов банка и снятие с указанных карточных счетов наличных денег через банкоматы;
- изготовление дубликатов карт, находящихся в пользовании держателя, и снятие наличных денег через банкоматы;
- присвоение списанных карт под видом испорченных, зачисление на них денежных средств с последующим снятием наличных денег через банкоматы;
- неправомерный доступ в компьютерную систему банка и последующая корректировка счета держателя карты в сторону уменьшения суммы снятых наличных денег;
- внесение изменений в компьютерную программу банкомата с последующим снятием наличных денег по многократно завышенному обменному курсу рубля.

В число подготовительных действий преступников с участием персонала банков в этой сфере входят:

- подыскание соучастников и распределение ролей в совершении преступления;
- разработка планов совершения и маскировки преступлений;
- создание вредоносной программы с целью получения возможности корректировки счета держателя карты;
- незаконное получение пароля для входа в компьютерную систему банкомата и программы ее перенастройки с целью завышения обменного курса одной из валют;
- незаконное получение и использование персональных данных о клиентах банка (в том числе бывших), на имя которых без их ведома оформляются кредитные карты;
- неправомерный доступ в компьютерную систему банка и последующие изменения телефонных номеров держателей карты на номера телефонов соучастников преступления с целью получения PIN-кода карты по телефону;
- перехват на почте карты, отправленной из головного офиса банка на адрес держателя;
- установление телефонной связи с оператором центрального офиса банка и получение кода доступа для активации карт под видом законного держателя.

В ряде случаев мошенники вовлекают в незаконное собирание и разглашение сведений о картах работников банков и организаций, имеющих непосредственный доступ к сети и базам данных

Основными способами хищения денежных средств со счетов держателей банковских карт без участия персонала банков являются:

- хищение денежных средств с использованием подлинных карты и кода идентификации, похищенных у держателя;
- хищение товаров в интернет-магазинах без предъявления подлинной карты, но с использованием сведений о ее реквизитах, незаконно полученных от держателя карты;
- хищение денежных средств с использованием поддельной карты, имитирующей внешний вид подлинной карты с нанесенными на ее магнитный носитель реквизитами подлинной карты;
- хищение денежных средств с использованием карты банка, выданной банком, однако подделанной путем перекодирования информации, содержащейся на магнитном носителе;
- хищение денежных средств с использованием кредитной карты, выданной мошенникам по поддельным паспорту и документу, подтверждающему его кредитоспособность;
- хищение денежных средств с использованием поддельной карты, не имеющей внешнего сходства с подлинными (так называемый белый пластик), однако снабженной магнитным носителем, содержащим реквизиты реального карточного счета.

Предупреждение хищений денежных средств банка с использованием пластиковых карт

Программы предупреждения хищений денежных средств банка с использованием пластиковых карт, как правило, содержат комплекс мер организационного и технологического характера.

Организация выпуска карт должна начинаться с письменного согласования определенных мер между подразделениями, участвующими в указанной процедуре. В процессе согласования инициатор выпуска готовит мотивированное предложение об изготовлении карт; бухгалтерия подтверждает факт наличия средств на выпуск карты; служба безопасности (защиты интересов банка) высказывает свое мнение о необходимых мерах защиты изготовления и использования карт; группа изготовления карт готовит предложения производственно-технологического характера. Эти меры направлены на предотвращение возможного несанкционированного выпуска карт.

В число **организационных мер** входит проведение предварительной проверки персональных данных будущих владельцев пластиковых карт и разработка рекомендаций для повышения надежности их хранения. Пристальное внимание соответствующих подразделений банка уделяется также проверке предполагаемых организаций-партнеров, предлагающих обслуживание клиентов банка по пластиковым картам.

Меры технологического характера имеют своей целью повышение надежности процедуры передачи информации платежной системы и идентификации владельца карты.

Этому способствует внедрение так называемых смарт-карт (от англ. *smart card*) – платежных карт со встроенным микропроцессором, обеспечивающим качественно новый уровень защиты содержащейся в ней информации. Зарубежные банки, в частности, внедряют идентификационные системы с использованием биометрических (голос, отпечатки пальцев рук и др.) параметров держателей карт.

Самостоятельными направлениями являются обеспечение мер безопасности в процессе изготовления карт и их рассылки: сохранности изготовленных карт, их заготовок и расходных материалов; соблюдение требований по разделению уровней доступа к различным этапам изготовления карт с целью предельного ограничения числа лиц, осведомленных о вносимой в карту ключевой информации.

Система контроля за операциями с пластиковыми картами реализуется в двух направлениях: внешнем и внутреннем. Первое направление призвано отслеживать операции с пластиковыми картами вне банка. В число его задач входит, в частности, ведение и публикация специального банковского реестра с номерами заблокированных пластиковых карт (стоп- листа).

Задача второго направления – вести контроль за расчетами непосредственно в подразделениях, осуществляющих выпуск пластиковых карт и расчеты с их использованием.

Технические средства защиты от хищений денежных средств банка путем незаконного использования пластиковых карт включают в себя:

- средства защиты карт от несанкционированного использования;
- средства защиты процессинговых центров, обрабатывающих операции с картами;
- средства защиты банкоматов для выдачи наличных денег.

Технико-криминалистические средства выявления, предупреждения и пресечения хищений в процессе использования пластиковых карт позволяют выявлять описанные выше признаки подделки карт и личных документов их держателей.

Основные способы хищения денежных средств с использованием систем удаленного управления счетом ("Банк-Клиент" и "Интернет-банкинг")

Для совершения хищений с использованием систем удаленного управления счетом мошенники создают и авторизуют полностью поддельное электронное платежное сообщение или искажают реквизиты реально существующего платежного сообщения.

Для совершения хищений *со счетов юридических лиц* преступные группы с участием персонала банка (и персонала организации-клиента), как правило, выполняют следующие подготовительные действия:

- незаконное завладение паролем-ключом к электронной системе "Банк-Клиент" работником организации;
- создание и использование вредоносных компьютерных программ с целью незаконного получения информации о ключах и паролях банковских систем управления счетами;
- создание и использование вредоносных компьютерных программ с целью их внедрения в компьютеры клиентов для незаконного получения информации о ключах и паролях доступа к системе дистанционного обслуживания счета;
- незаконное получение информации о паролях клиентов систем "Интернет-банкинг" от так называемых информационных брокеров (путем личного контакта либо безличного общения через Интернет);
- неправомерный доступ к охраняемой законом компьютерной информации банка, обеспечивающей платежный технологический процесс;
- неправомерный доступ к охраняемой законом компьютерной информации клиента банка, обеспечивающей платежный технологический процесс;
- создание лжекоммерческой организации и открытие ее банковского счета, на который планируется перевести похищенные денежные средства;
- открытие счета на собственное имя или имя родственников с целью последующего перевода похищенных денежных средств;
- открытие счета на имя подставного физического лица с целью последующего перевода похищенных денежных средств;
- оформление зарплатных карт на имя мнимых работников фиктивных организаций с целью получения наличных денег.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1

Заполните таблицу «Элементы защиты банковских карт»

Элементы	Назначение
Пин-код	
Магнитная полоса на обратной стороне карты.	
Электронный чип	
Коды CVC2 или CVV2.	
Голограммы и иные защитные элементы на карте.	
Подпись владельца на обратной стороне карты.	
СМС-информирование клиента о транзакциях.	

Задание 2

Можно ли списать денежные средства с банковской карточки, не зная Пин –код? Ответ аргументируйте.

Задание 3

Назовите плюсы и минусы Использование технологии SMS-информирования держателей банковских карт.

Задание 4

Перечислите наиболее эффективные меры предосторожности при расчётах банковскими картами в Интернете

Задание 5

Выберите правильный ответ

Скимминг-это.

1 Попытка предъявления к оплате потерянной владельцем или украденной у него карты.

2. Кража карточных данных при совершении операций в банкомате путем установки считывающих устройств,

3. Использование специальных приспособлений для блокировки пластиковой карты в банкоматах
Как банки борются со скиммингом?

Задание 6

Владелец счета получает письмо, якобы из банка, где ему предлагается пройти по указанной ссылке. На специально созданном сайте, интерфейс которого, скорее всего, будет очень похож на настоящий банковский, его уже ждет подробная инструкция и окошечки для ввода конфиденциальной информации.

Как называется данный метод мошенничества? Предложите возможные меры защиты от него.

Задание 7

NFC карты – интересное новшество, позволяющее расплачиваться за осуществленную покупку без контакта платежной карточки с терминалом. Необходимо только поднести карту на расстояние 2-5 см от терминала и оплата за приобретенный товар либо услугу поступит на нужный счет.

Когда речь идет о том, насколько безопасны бесконтактные карты PayWave сегодня, представители банков России всегда говорят о том, что случаев, когда средства со счета были украдены, еще не наблюдалось. Это действительно так. Как вы прокомментируете данный факт ? Действительно ли, так безопасны бесконтактные карты PayWave .

Задание 8

Используя систему «Консультант Плюс Составить таблицу

Таблица 1 Способы мошенничества с пластиковыми картами

Способы мошенничества	Виды преступлений	Законодательная база и предусмотренное наказание
Хищение с использованием подлинных карт, утраченных владельцами		
Хищение с использованием поддельных карт		
Хищения с использованием подлинных карт, оформленных злоумышленниками в установленном порядке		

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1 Что входит в число основных способов хищения персоналом банков денежных средств в сфере обслуживания держателей банковских карт?

2 Перечислите основные способы хищения денежных средств со счетов держателей банковских карт без участия персонала банков ?

3 Перечислите меры предупреждения хищений денежных средств банка с использованием пластиковых карт.

4 Перечислите основные способы хищения денежных средств с использованием систем удаленного управления счетом ("Банк-Клиент" и "Интернет-банкинг")

Практическая работа № 4 Действия службы безопасности и сотрудников банка в кризисных ситуациях.

ЦЕЛЬ РАБОТЫ формирование практических умений анализировать кризисные ситуации в банке и навыков действий в кризисных ситуациях.

Для выполнения работы необходимо **знать** организационные основы банковской деятельности, функции подразделений безопасности банков, вопросы соблюдения прав и свобод личности при решении задач обеспечения безопасности ; необходимо **уметь** оценивать степень угрозы личной безопасности банковского специалиста; анализировать кризисные ситуации в банке; действовать при возникновении кризисной ситуации в банке.

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Кризисная ситуация - это всегда угроза для безопасности компании, как репутационной, так и финансово-экономической.

Кризис – это неожиданный случай или ряд событий, выходящих из-под контроля, прерывающих нормальное функционирование организации и вызывающее настойчивое и нежелательное общественное внимание, которое вредит или угрожает нанести вред репутации организации.

К типичным признакам кризисной ситуации в первую очередь относится появление негативных публикаций в СМИ и участвовавшие проверки государственными органами контроля и надзора, явно спровоцированные конкурентами.

Кризисные ситуации, возникающие в организации, могут быть классифицированы на следующие виды:

■ Технологические кризисы - кризисы, вызванные несовершенством применяемых технологий. Их результатом являются сбои в работе, аварии и как следствие - ухудшение позиций компании на рынке.

■ Конфронтационные кризисы - обострение противостояния соперничающих участников рынка, в результате чего возможен бойкот выпускаемых продуктов и предлагаемых услуг. ■ Кризисы злонамеренного поведения - возможная террористическая опасность.

Кризисы менеджмента - кризисные ситуации, спровоцированные неверными управленческими решениями или несовершенством системы их внедрения.

В зависимости от динамики протекания кризисы можно подразделить на следующие виды:

1. Неожиданные кризисы (происходят внезапно, требуют заблаговременного общего плана действий);
2. Назревающие кризисы (дают больше времени для изучения и планирования, но вступают в разрушительную стадию внезапно, важно предпринять шаги до этого момента);
3. Непрерывные кризисы (длятся месяцами и даже годами, часто поддерживаются очередной волной слухов).

В зависимости от вида кризиса определяется тип антикризисного PR. Антикризисный PR – комплекс мероприятий по прогнозированию, недопущению или преодолению кризиса репутации. В целом антикризисный PR - это комплекс высокоэффективных технологий, ориентированных на прогнозирование, выявление и предотвращение кризиса, управление им и выход из него, а также регулирование его последствий. Сюда же относятся методики поддержания и оперативной коррекции имиджа, адаптации к новым условиям, нейтрализации негативных технологий.

Поведение людей во время кризиса называется «кризисным поведением». Примером такого поведения может служить паника. Последствия паники могут быть гораздо более разрушительными, чем причины ее вызвавшие. Другим примером «кризисного поведения» может служить оцепенение, либо апатия. К сожалению, «кризисное поведение» «заразно». Оно передается от сотрудника к сотруднику, от организации к организации и даже от страны к стране. Одной из причин «кризисного поведения» на уровне организации может служить недостаток информации и отсутствие четкого плана действий.

Компаниям следует обязательно проводить деятельность по планированию кризиса. Важно заранее выработать общие принципы и стратегию антикризисной коммуникационной программы, к которой компания обратится в случае возникновения кризиса. А если кризис не удалось предотвратить, то следует занять четкую недвусмысленную позицию - достаточно гибкую, но принципиальную. Централизовать коммуникации (только один представитель компании имеет право делать официальные заявления). Привлечь к активным действиям руководство. Постоянно поддерживать связи со СМИ. Подключить «внешнюю группу поддержки» (специалистов, лидеров мнений, клиентов, потребителей, ученых, чиновников, представителей общественных организаций). Не игнорировать своих работников - они должны быть проинформированы о сути ситуации и позиции компании в первую очередь. Осуществлять постоянный мониторинг и оценку протекания кризиса. Заранее думать о позиционировании компании после кризиса.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1 Составьте перечень возможных кризисных ситуаций в банковской деятельности.

Задание 2 Как вы понимаете фразу: Обиженный сотрудник-это мина замедленного действия, которая рано или поздно сработает.

Задание 3

В интернете появилась информация о возможном отзыве лицензии у крупного банка. У клиентов началась паника. Предложите меры, которые позволят на ваш взгляд поддержать необходимый уровень дисциплины и порядка

Задание 4

Перечислите психологические факторы низкой надежности персонала. Как они могут отразиться на безопасности банка? Предложите способы предупреждения и выявления ненадежности персонала

Задание 5 Составьте таблицу «кризисного поведения» сотрудников банка и предложите меры, которые позволят на ваш взгляд поддержать необходимый уровень дисциплины и порядка.

Задание 6 Составьте инструктаж по технике безопасности:

А При нападении на банк и захвате заложников

Б При обнаружении подозрительных предметов или угрозе взрыва.

Задание 7* По материалам периодических изданий и сайтов интернет подготовьте доклад о действиях службы безопасности и сотрудников банка в кризисных ситуациях

КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1 Какую ситуацию можно считать кризисной для компании (банка)?
- 2 Какие признаки характерны для кризисной ситуации?
- 3 На какие виды могут быть классифицированы кризисные ситуации?
- 4 Какое поведение сотрудников компании (банка) можно отнести к кризисному
- 5 Причины кризисного поведения сотрудников?
- 6 Перечислите меры борьбы с кризисным поведением сотрудников?

Практическая работа № 5 Противдействие легализации(отмыванию)доходов, полученных преступным путем, и финансирование терроризма.

ЦЕЛЬ РАБОТЫ формирование практических навыков выявления проводимых клиентами коммерческого банка операций, связанных с легализацией доходов.

Для выполнения работы необходимо **знать** организационные основы банковской деятельности, функции подразделений безопасности банков, вопросы соблюдения прав и свобод личности при решении задач обеспечения безопасности;; необходимо **уметь** выявлять попытки финансирования преступлений

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Под **легализацией (отмыванием) доходов**, полученных преступным путем, в Российском законодательстве понимается совершение действий, направленных на придание правомерного вида владению, пользованию и распоряжению денежными средствами и иным имуществом, приобретенным заведомо незаконным путем и полученным от таких видов преступлений, как незаконная торговля наркотиками, создание фирм-однодневок, финансовые мошенничества и другие действия.

Легализация преступных доходов представляет собой сложный процесс, включающий множество разнообразных сделок, совершаемых разнообразными методами.

Такое явление способствует дальнейшему росту преступности не только экономической направленности, но и иной, в том числе организованной (отмывание доходов, полученных преступным путем, является одним из элементов организованной преступной деятельности и выступает финансовым рычагом террористической деятельности).

Основные цели легализации доходов, полученных преступным путем

- Соккрытие источников и характеров происхождения средств.
- Формирование видимости легальности имеющихся доходов.
- Соккрытие лиц, которые являются владельцами нелегальных доходов и занимаются их отмыванием.
- Уклонение от перечисления налогов.
- Формирование беспрепятственного доступа к деньгам.
- Формирование условий для безопасного использования средств.
- Создание возможности для свободного инвестирования в законный бизнес.

Выделяются следующие способы отмывания доходов, добытых преступным путем:

1. Неоправданное завышение стоимости услуг и продукции.
2. Заключение соглашений с фиктивными организациями с последующими переводами на счета крупных сумм средств. Полученные средства направляются на законную деятельность.
3. Нелегальные операции по обезличиванию и обличиванию средств через банковское учреждение, фиктивные фирмы.
4. Формирование видимости получения кредитных средств от банковского учреждения или организации-нерезидента, оформленной в оффшорной зоне. Создается эта видимость путем множественного перечисления безналичных средств на счета разных компаний. После этого средства возвращаются обратно.
5. Проведение сделок и банковских операций через оффшорные компании, созданные банковским учреждением. Сделки могут осуществляться через финансовые фирмы, которые не являются аффилированными. Признаки этого способа отмывания: сделки с компаниями, зарегистрированными в оффшорных зонах, фиктивные переводы средств в форме кредита на счета банковского учреждения, не являющегося резидентом. Затем средства переводятся в другой оффшорный банк. После этого средства возвращаются обратно. Сложная сеть операции нужна для того, чтобы скрыть источник поступления средств.

6. Пересылка средств в другую страну, из другой страны или на территории одного государства. Сюда относятся международные переводы. К примеру, это может быть перевод средств в другую страну для приобретения недвижимости.
7. Направление средств, которые ранее переведены на зарубежные счета, на инвестирование в РФ. Это может быть приобретение ценных бумаг крупных предприятий. Этот способ крайне распространен. Связано это с тем, что огромные объемы нелегальных средств хранятся именно на зарубежных счетах. Тратить средства в этих же странах сложно, так как легко отслеживается их преступное происхождение. Поэтому средства возвращаются в РФ. Самый простой способ возврата – приобретение акций.
8. Создается фиктивное предприятие. Доход от преступной деятельности оформляется как законная прибыль этого предприятия. В качестве этого предприятия может быть создан, к примеру, кинотеатр, ресторан.

Для обеспечения эффективного противодействия легализации преступных доходов в банковской сфере разработан комплекс мер и мероприятий, нацеленных на выявление проводимых клиентами банка «подозрительных» операций. В связи с этим первоочередной задачей банка является адекватное восприятие специфики таких операций, и безошибочное выявление их возможной связи с легализацией доходов полученных преступным путем и предотвращение любых финансовых сделок прямо или косвенно связанных с незаконной деятельностью и/или ее финансированием.

Деятельность банка подразумевает сбор информации о клиентах банка и проводимых ими финансовых операциях. Основная цель данной программы состоит в получении банком информации о клиенте и его деятельности еще на стадии первичного обращения в банк. Полученная в результате проверки информация используется как для оценки рисков проведения клиентом в дальнейшем операций по легализации денежных средств, так и для проведения других программ, направленных на обеспечение безопасности банка. Сбор информации осуществляется как в отношении юридических, так и в отношении физических лиц. В обоих случаях, источниками информации становятся как данные, предоставленные клиентом при заполнении анкеты, так и данные, содержащиеся в полученных от него документах. Анализ информации включает в себя анализ регистрационных сведений, вида деятельности (занятости), анализ информации учредительного и организационно-структурного характера для клиентов-юридических лиц.

- Также банки занимаются изучением, анализом, структурированием и хранением ранее собранной информации. Собранная информация сохраняется банком в отдельном помещении, исключающим несанкционированный доступ, и хранится в досье клиента, которое банк открывает в момент первого обращения. Содержимое данных досье клиента является конфиденциальной информацией и не подлежит разглашению. Закрывание досье проводится при прекращении обслуживания клиента в банке, либо по истечении трех календарных лет с момента последнего обращения клиента в банк.

- Банк также занимается выявлением проводимых клиентами операций, связанных с легализацией доходов, полученных нелегальным способом. Выявление клиентов, связанных с такого рода деятельностью проводится по двум основным направлениям. Во-первых, контроль осуществляется применительно к списку операций, подлежащих обязательному контролю, согласно ст.6 Федерального Закона № 115-ФЗ от 07.08.2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем» и осуществляется сотрудниками отделов клиентского обслуживания, анализирующими сведения, представляющие собой параметры и условия проведения операции, на соответствие разработанным для этих целей критериям. Во-вторых, проводимые клиентами банков операции ежедневно проверяются на наличие «подозрительных» (т.е. обладающих определенными признаками). Мониторинг проводится как сотрудниками банка, так и автоматически, и предполагает проверку сведений, полученных от правоохранительных и иных уполномоченных органов, проведение в обязательного контроля деятельности клиента банка, а также мониторинг средств массовой информации.

- В тех случаях, когда клиент признан «подозрительным», уровень риска от проведения сделок с ним определяется как «высокий», и его деятельность подлежит тщательной проверке с целью сбора более детальной информации о деятельности клиента и проводимых им финансовых

операциях. Основная задача данной проверки - подтвердить обоснованность подозрений или полностью опровергнуть их. Проверка проводится в течение определенного времени и с определенной периодичностью (как правило, не реже одного раза в полгода) по мере накопления необходимой информации о самом клиенте и о проводимых им финансовых операциях. Методы анализа и критерии, применяемые для оценки результатов, как правило, определяются отдельно для каждого случая проверки, а полученные сведения сохраняются в досье клиента.

- Также в обязанности банка входит взаимодействие с органами финансового надзора в соответствии с законодательством по противодействию легализации доходов, полученных преступным путем.

Обязанность организовать функционирование подсистемы финансового контроля возложена Законом о противодействии отмыванию доходов (ст. 8) на уполномоченный орган – Федеральную службу по финансовому мониторингу (Росфинмониторинг). Названная служба является федеральным органом исполнительной власти, осуществляющим функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма и координирующим деятельность в этой сфере иных федеральных органов исполнительной власти.

Функции методического руководства и координации деятельности кредитных организаций отнесены к компетенции Банка России.

Финансовый контроль осуществляется в целях сбора информации, необходимой для выявления фактов противоправной деятельности, их предварительной проверки, оценки и возможного направления материалов в правоохранительные органы, которые рассматривают поступившие материалы финансового контроля в качестве основания для принятия по ним решения в рамках УПК РФ.

Законодательство не устанавливает административной ответственности за совершение сделок и операций, направленных на легализацию (отмывание) преступных доходов. Однако неисполнение банком предписаний Закона о противодействии отмыванию доходов в части фиксирования, хранения и представления информации об операциях, подлежащих обязательному контролю, а также в части организации внутреннего контроля рассматривается как административное правонарушение и служит основанием для наложения административного штрафа.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1

Опишите схему легализации доходов

А при незаконном получении кредита

Б при создании фиктивной фирмы

В Осуществление конверсионных операций, связанных с обменом валюты.

Задание 2

Определите какие из операций подлежат обязательному контролю?

В операционной кассе банка были проведены следующие операции с иностранной валютой:

Продажа 5 000 долларов США

Покупка 15 000 евро

Покупка 20 000 долларов США

Внесено во вклад физического лица 15 000 долларов США

Курсы валют коммерческим банком на дату совершения операции:

Покупка доллара США 58,62 Продажа доллара США 62,90

Покупка евро 60,20 Продажа евро 65,30

Задание 3

Ознакомьтесь со ст.6 Федерального Закона № 115-ФЗ от 07.08.2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем» .

Проанализируйте ситуации. Определите, подлежат ли данные операции обязательному контролю? Какие должны последовать действия сотрудника банка при проведении данных операций ?

Ситуация 1. Клиент проводит операцию по оплате налоговых платежей, которую он совершает наличными деньгами на общую сумму 40 000 рублей. При введении сотрудником кредитной организации идентификационных данных клиента в программу банка по проведению платежей, машина высветила информацию, что данный клиент находится в списках экстремистов и террористов.

Ситуация 2. Физическое лицо обратилось в банк с просьбой разменять 100 долларовые купюры на общую сумму 15000 долларов США на более мелкие (по 10 долларов). Курс Банка России на дату совершения операции 58.73 руб. за 1 долл. США.

Ситуация 3 Юридическое лицо представило в банк чек для снятия наличными 650 000 рублей с целью покупки оборудования для строительных работ. В то же время из учредительных документов клиента следует, что данное предприятие создавалось с целью оказания услуг населению по ремонту и чистке одежды. Кроме того, операции, которые ранее совершал клиент, не относились к операциям, связанным с каким-либо строительством.

Ситуация4 Клиент физическое лицо открыл вклад на свое имя на сумму 630 000 рублей, а через 7 дней закрыл вклад?

Ситуация5 Клиент физическое лицо открыл вклад в банке в пользу другого физического лица с внесением во вклад наличных денежных средств в размере 700 000 рублей.

Задание 4

Ответьте на вопросы теста

№п/п	Вопрос/Задание	Варианты ответа
1	ФСФМ РФ (Росфинмониторинг) является:	А Федеральным органом законодательной власти Б Структурным подразделением Банка РФ В Федеральным органом исполнительной власти
2	Является ли предоставление информации в ФСФМ РФ нарушением Банковской или иной тайны	А Является нарушением банковской тайны Б является нарушение служебной тайны В Не является нарушением какой-либо тайны.
3	Имеет ли право сотрудник провести операцию по открытию вклада в пользу третьих лиц с размещением в него денежных средств в наличной форме на сумму 600 000 рублей?	А Не имеет Б Имеет В Операция подлежит обязательному контролю и проводится с разрешения Ответственного сотрудника Банка
4	Идентификацию каких из указанных лиц должен осуществлять Банка при проведении банковских операций?	А Клиентов кредитной организации Б Контрагентов клиентов кредитной организации В Всех указанных лиц

5	5 Как часто следует информировать клиента о сообщениях, предоставляемых в ФСФМ РФ в отношении операций клиента	А По письменному запросу клиента Б По каждой операции В Клиента информировать запрещено
6	Документами удостоверяющими личность, для гражданина РФ являются:	А Паспорт гражданина РФ Б Общегражданский заграничный паспорт В Паспорт моряка Г Все выше указанные документы являются документами, удостоверяющими личность
7	Подлежит ли направлению в уполномоченный орган сообщение о сделке, признанной подозрительной, на сумму 590 000 рублей?	А Нет, не подлежит. Сумма операции меньше 600 000 рублей, следовательно, сообщение не направляется Б Да , подлежит, т.к. суммовой порог подобных операций не установлен В Да, подлежит, если предметом сделки –недвижимость
8	Какие из нижеперечисленных категорий лиц относятся к ИПДЛ?	А Главы государств или правительств Б Министры ,их заместители и помощники В Высшие правительственные чиновники Г Все вышеперечисленные категории лиц
9	Доходы, полученные преступным путем ,это:	А Доходы от операций с денежными средствами или иным имуществом,подлежащих обязательному контролю Б Доходы от операций с денежными средствами или иным имуществом,попадающих под категорию необычных В Денежные средства или иное имущество ,полученные в результате совершения преступлений
10	В каком случае покупка физическим лицом наличной иностранной валюты подлежит обязательному контролю	А В любом случае Б В случае,если сумма операции эквивалентна 15 000 рублей или превышает её ВВ случае,если сумма операции эквивалентна 600 000 рублей или превышает её
11	Минимальная сумма сделки с недвижимым имуществом, которая подлежит обязательному контролю	А 600 000 рублей Б 1000 000 рублей В 3 000000 рублей
12	По какому курсу определяется сумма операций в целях ее квалификации	А По курсу Банка России, действующему на дату совершения операций.

	как подлежащей обязательному контролю:	Б По текущему курсу Банка на дату совершения операции В По средневзвешенному курсу, сложившемуся на биржевом рынке на дату совершения операций.
13	Наличие каких сведений в отношении клиента Банк должен проверить в обязательном порядке?	А Сведений об уплате налогов Б Сведений о присутствии в руководящих органах клиента лиц с уголовным прошлым В Сведений об их участии в экстремистской деятельности
14	Чем руководствуется сотрудник Банка при выявлении необычных операций?	А Характером сделки Б Сложившейся банковской практикой проведения осуществляемой операции В Экономическом смысле проводимой операции Г Всеми указанными видами информации
15	Когда (на каких этапах) Банк осуществляет процедуру проверки клиентов на причастность к экстремистской деятельности?	А При установлении договорных отношений Б При проведении банковских операций В На всех указанных этапах
16	Чем должен руководствоваться сотрудник Банка с точки зрения ПОД/ФТ	А Правилами внутреннего контроля Банка в целях ПОД/ФТ Б Требованиями и рекомендациями Банка России по ПОД/ФТ В ФЗ №115-ФЗ Г Всеми вышеперечисленными документами
17	На какую сумму подлежит обязательному контролю операции ,если в отношении одного из участников операции имеются сведения о его участии в экстремистской деятельности?	А Не менее 2000 долларов США или эквивалент в рублях Б Для выявления таких операций суммовой порог не определен В 600 000 рублей, или эквивалент в иностранной валюте
18	Какие операции по своему характеру относятся к операциям обязательного контроля:	А Операция клиента не имеет явного экономического смысла Б Несоответствие операции клиента общепринятой практике совершения операций В Во всех случаях операции соответствуют критериям обязательного контроля Г Ни в одном из перечисленных случаев операции не соответствуют критериям обязательного контроля, но могут быть признаны необычными операциями.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

- 1 Что понимается под легализацией. доходов, полученных преступным путем?
- 2 Основные цели легализации доходов, полученных преступным путем?
- 3 Перечислите способы отмывания доходов, добытых преступным путем
- 4 Какие меры предпринимаются банками для обеспечения эффективного противодействия легализации преступных доходов в банковской сфере ?
- 5 Какова роль Федеральной службы по финансовому мониторингу (Росфинмониторинг), в противодействии легализации доходов, полученных преступным путем

Практическая работа №6 Использование технических средств в целях защиты банковской тайны.

ЦЕЛЬ РАБОТЫ Формирование практических умений и навыков по классификации и характеристике технических средств в целях защиты банковской тайны

Для выполнения работы необходимо *знать* технические и инженерно-технические средства защиты информации; необходимо *уметь* применять необходимые методы и средства защиты банковской информации, соблюдать, правила информационной безопасности банковских систем;

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Разработка и реализация практических мер по организации защиты банковской тайны в соответствии с действующим законодательством возлагается на ее обладателя. Именно он должен создать систему защиты сведений, составляющих банковскую тайну и иную информацию ограниченного доступа, и обеспечить ее эффективную работу.

Цель функционирования указанной системы – обеспечить оптимальный режим работы организации с таким расчетом, чтобы сделать информацию и сведения ограниченного доступа недостижимыми для посторонних лиц и создать необходимые условия работы сотрудникам, имеющим к ним доступ. Для этого устанавливается единый порядок работы с защищаемой информацией. Основная особенность этого порядка заключается в организации конфиденциального делопроизводства, принятии работниками обязательства строгого исполнения его правил и индивидуальной ответственности за обеспечение сохранности доверенных сведений ограниченного доступа и их носителей.

В рамках системы организуется обучение работников правилам соблюдения банковской тайны. Осуществляется систематический контроль за исполнением организационно-распорядительных документов и инструкций по обеспечению конфиденциальности информации. Система предусматривает наличие типовой процедуры анализа и разбирательства (ведомственного расследования) по фактам нарушения порядка работы со сведениями, составляющими банковскую тайну, и выработку предложений по совершенствованию защиты информации.

Особенности организации защиты информации, составляющей коммерческую тайну, от утечки по техническим каналам. Главной задачей этой деятельности является создание системы защиты информации ограниченного доступа, циркулирующей в технических средствах и помещениях, от утечки и умышленного перехвата с противоправными целями. Такая система должна состоять из двух блоков: технического и функционального. В рамках первого ведется разработка и внедрение технических средств защиты информации, циркулирующей в средствах техники и связи.

С указанной целью технической защитой обеспечиваются:

- – помещения, предназначенные для ведения конфиденциальных переговоров;
- – средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства), средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видеосмысловой и буквенно-цифровой информации, программные средства (операционные системы, системы управления базам и данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки информации ограниченного доступа;

- – технические средства и системы, не обрабатывающие непосредственно информацию ограниченного доступа, но размещенные в помещениях, где обрабатывается (циркулирует) такая информация (с целью предупредить незаконное получение информации ограниченного доступа путем перехвата акустического, электрического, электромагнитного, вибрационного и других видов излучений, возникающих при обработке информации техническими средствами);
- – радиоизлучения или электрические сигналы от внедренных в технические средства и помещения специальных электронных устройств перехвата информации ("закладок");
- – радиоизлучения или электрические сигналы от устройств перехвата информации, подключенных к каналам связи, а также к отдельным носителям информации.

Кроме того, технические средства защиты информации от утечки должны препятствовать непреднамеренному попаданию сведений ограниченного доступа к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Например, вследствие прослушивания разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции стен, систем вентиляции и кондиционирования воздуха; случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС; просмотра информации с экранов дисплеев и других средств ее отображения через двери и окна.

Решение технических задач возлагается на подразделения (либо отдельных специалистов) разработки технических средств защиты информации.

Другой важной задачей создания системы защиты информации является организация функционирования указанных выше технических и программных средств в определенном режиме. Ее решение требует принятия пакета организационно-распорядительных и рабочих документов. В частности, издания приказов о создании соответствующих подразделений по защите информации и назначении лиц, ответственных за эксплуатацию технологического оборудования и электронных банков данных.

Созданные подразделения, в свою очередь, готовят совместно с разработчиками средств технической защиты инструкции с описанием требований по защите информации, которые должны выполнять в процессе обработки (передачи) информации лица, ответственные за эксплуатацию технологического оборудования и электронных баз данных, пользователи информации ограниченного доступа и сотрудники подразделений по защите информации.

Программа обеспечения функционирования системы защиты информации ограниченного доступа должна включать в себя выполнение специальной проверки технических средств и служебных помещений на предмет отсутствия в них возможно внедренных электронных устройств перехвата информации ("закладок"); организацию охраны и физической защиты объекта информатизации и отдельных технических средств, исключающих несанкционированный доступ к ним, а также контроль состояния и эффективности защиты информации.

В целях предупреждения внедрения "закладок" в технические средства и интерьер подразделения по защите информации составляет технический паспорт на каждое защищаемое помещение. Этот документ должен содержать план размещения оборудования и схему его кабельных соединений. В паспорт включается перечень оборудования и мебели, установленных в помещении, с указанием типа, учетного или инвентарного номера и даты установки и замены. Кроме того, в нем отражаются перечень реализованных мероприятий по защите информации, даты и результаты периодических проверок системы защиты.

Детальные описания порядка осуществления работ, основные требования и рекомендации, способы и средства защиты информации, циркулирующей в технических средствах и помещениях, изложены в документе под названием "Специальные требования и рекомендации по технической защите конфиденциальной информации"[1].

Задача обеспечения защиты информации от утечки по техническим каналам, как и во всех иных указанных выше случаях, возлагается на руководителей организации и подразделений, которые разрабатывают и эксплуатируют объекты информатизации, организуют и осуществляют защиту информации (службы безопасности).

Однако в случае необходимости руководитель организации может привлечь на договорной основе для разработки средств защиты информации и проведения мероприятий по ее защите специализированные учреждения и предприятия, имеющие лицензию на право осуществления указанных видов деятельности. Контроль за соблюдением правил эксплуатации системы защиты

информации, ее состоянием и эффективностью защиты информации осуществляется подразделениями по защите информации предприятия-заказчика.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1

Составьте кластер «Классификация технических средств защиты банковской тайны»

Задание 2

Для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1 виды угроз;

2 источники появления угроз;

3 какие технические средства защиты можно использовать?

Наименование объекта защиты информации:

а) Одиночно стоящий компьютер в бухгалтерии.

б) Почтовый сервер.

в) Телефонная сеть.

г) Средства телекоммуникации (радиотелефоны, мобильные телефоны)

д) Банковские операции (внесение денег на счет и снятие).

е) Операции с банковскими пластиковыми карточками.

ж) Компьютер, хранящий конфиденциальную информацию о сотрудниках банка

з) Компьютер, хранящий конфиденциальную информацию о клиентах банка

и) Комната для переговоров по сделкам на охраняемой территории.

Задание 3

Заполните таблицу «Технические средства охраны»

Инженерно-технические средства охраны»	Назначение
Система охранно-пожарной сигнализации	
Система тревожной сигнализации	
Система оповещения	
Телевизионная система наблюдения	
Химические ловушки	
Полиграф	

Задание 4*

По материалам периодических изданий и сайтов Интернет подготовить доклад о современных технических средствах защиты банковской тайны

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1 На кого возлагается Разработка и реализация практических мер по организации защиты банковской тайны?

2 Что относится к техническим средствам защиты ?

3 Что относится к инженерно-техническим методам защиты?

4 На кого возлагается задача обеспечения защиты информации от утечки по техническим каналам?

5 Что включает в себя программа обеспечения функционирования системы защиты информации ограниченного доступа ?

Литература:

Основная литература:

1. Безопасность банковской деятельности :учеб.пособие/ В.В.Цой, М.М. Лукьянчук; СПб банковский колледж Банка России.-СПб.:Изд-во «Лема»,2016.-175с.

Интернет - ресурсы

1. Информационная безопасность банков. Отраслевой портал [Электронный ресурс]. – Режим доступа: <http://www.ib-bank.ru>.

2. Информационная безопасность организаций банковской системы Российской Федерации [Электронный ресурс]. Режим доступа: <http://www.cbr>

