МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И СЕРВИСА

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ ПО ПОЛУЧЕНИЮ НАВЫКОВ ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Информационная безопасность банковских систем РФ

Студент
гр. БЭП-21-ЭБ1 _____ Н.Н. Николашкин

Руководитель
канд. техн. наук,доцент _____ В.Н. Макарова

Владивосток 2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на учебную практику по получению навыков исследовательской работы

Студенту Николашкин Николай Николаевич группы БЭП-21-ЭБ1
(ФИО обучающегося полностью)
Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем
Место прохождения практики: ФГБОУ ВО «ВГУЭС», МИОСТ, КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Срок прохождения практики с «07» февраля 2023 г. по «25» июня 2023 г.

Содержание отчета по практике:

Задание 1. Анализ поставленной задачи

- развернутое описание поставленной задачи с точки зрения ее актуальности, истоков возникновения проблемы, возможных форм проявлений и последствий (УК-1.3);
- анализ содержания проблемы с точки зрения сфер, которые она затрагивает (социальная, экономическая, политическая и т.п.) (УК-1.3);
- разбивка поставленной цели исследования на задачи, разработка плана исследования, выбор методов исследования (УК-1.3).

Задание 2. Сбор и анализ информации

- определение перечня информации/данных, необходимых для анализа и поиска решения поставленной задачи (УК-1.3);
- определение источников необходимой информации/данных (УК-1.1);
- сбор и систематизация информации/данных (УК-1.1).

Задание 3. Разработка решения поставленных задач

- формулировка выводов и заключений по результатам проведенного анализа информации (УК-1.3);
- разработки и обоснования решений поставленных задач на основе полученных результатов исследования (УК-1.3);
- определение возможных направлений дальнейших исследований анализируемой проблемы (УК-1.1).

Задание 4. Оформить отчет и документы практики в печатном и электронном виде и представить на защиту в соответствии с требованиями организации и в установленные графиком практики сроки.

Отчет должен быть оформлен в соответствии с предъявляемыми требованиями стандарта ВГУЭС СК-СТО-ТР-04-1.005-2015 «Требования к оформлению текстовой части выпускных квалификационных работ, курсовых работ (проектов), рефератов, контрольных работ, отчетов по практикам, лабораторным работам».

Руководитель практики
канд.техн.наук, доцент кафедры туризма и экологии _____ В.Н. Макарова
Задание получил студент _____ Н.Н. Николашкин
«07» февраля 2023 г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАЛЕНДАРНЫЙ ПЛАН-ГРАФИК

Студент *Николашкин Николай Николаевич* группы БЭП-21-ЭБ1

направляется для прохождения учебной практики по получению навыков исследовательской работы

Срок прохождения практики с «07» февраля 2023 г. по «25» июня 2023 г.

Содержание выполняемых работ	Сроки исполнения		Заключение и оценка руководителя практики	Подпись руководителя практики
	начало	окончание		
Анализ поставленной задачи	07.02.2023	18.02.2023		
Сбор и анализ информации	19.02.2023	19.05.2023		
Разработка решения поставленных задач	20.05.2023	11.06.2023		
Оформление отчета и сдача руководителю практики от кафедры	12.06.2023	23.06.2023		
Защита отчета	24.06.2023	25.06.2023		

Студент-практикант _____ Н.Н. Николашкин

Руководитель от кафедры _____ В.Н. Макарова

Содержание

Введение

Со времен своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. В настоящее время в результате повсеместного распространения электронных платежей, пластиковых карт, компьютерных сетей объектом информационных атак стали непосредственно денежные средства как банков, так и их клиентов. Совершить попытку хищения может любой - необходимо лишь наличие компьютера, подключенного к сети Интернет. Причем для этого не требуется физически проникать в банк, можно «работать» и за тысячи километров от него.

Именно эта проблема является сейчас наиболее актуальной и наименее исследованной. Если в обеспечении физической и классической информационной безопасности давно уже выработаны устоявшиеся подходы (хотя развитие происходит и здесь), то в связи с частыми радикальными изменениями в компьютерных технологиях методы безопасности автоматизированных систем обработки информации банка (АСОИБ) требуют постоянного обновления.

Целью исследования является раскрытие вопроса информационной безопасности банков.

Поставленная цель определяет следующие задачи:

1. Систематизировать информацию о том, что такое Особенности информационной безопасности банков, что такое информационная безопасность банка.

2. Рассмотреть основные проблемы и задачи обеспечения защиты информации в условиях применения компьютерной технологии ведения банковского делопроизводства

При выполнении поставленных задач были использованы методы: анализа и обобщения данных учебной и научной литературы.

1 Теоретические аспекты процессов защиты информации

1.1 Особенности информационной безопасности банков

Банковская информация всегда была объектом пристального интереса всякого рода злоумышленников. Любое банковское преступление начинается с утечки информации. Автоматизированные банковские системы являются каналами для таких утечек. С самого начала внедрения автоматизированных банковских систем (АБС) они стали объектом преступных посягательств.

Так, известно, что в августе 1995 г. в Великобритании был арестован 24-летний российский математик Владимир Левин (рисунок 1), который при помощи своего домашнего компьютера в Петербурге сумел проникнуть в банковскую систему одного из крупнейших американских банков Citibank и попытался снять с его счетов крупные суммы. По сведениям московского представительства Citibank, до тех пор подобное никому не удавалось. Служба безопасности Citibank выяснила, что у банка пытались похитить $2,8 млн., но контролирующие системы вовремя это обнаружили и заблокировали счета. Украсть же удалось лишь $400 тысяч.

Рисунок 1 – Владимир Левин

В связи с этим, стратегия информационной безопасности банков весьма сильно отличается от аналогичных стратегий других компаний и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью банков, которые вынуждены делать доступ к счетам достаточно легким с целью удобства для клиентов.

Обычная компания строит свою информационную безопасность, исходя лишь из узкого круга потенциальных угроз - главным образом защита информации от конкурентов

(в российских реалиях основной задачей является защита информации от налоговых органов и преступного сообщества с целью уменьшения вероятности неконтролируемого роста налоговых выплат и рэкета). Такая информация интересна лишь узкому кругу заинтересованных лиц и организаций и редко бывает ликвидна, т.е. обращаема в денежную форму.

Информационная безопасность банка должна учитывать следующие специфические факторы: Хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги. На основании информации компьютера могут производиться выплаты, открываться кредиты, переводиться значительные суммы. Вполне понятно, что незаконное манипулирование с такой информацией может привести к серьезным убыткам. Эта особенность резко расширяет круг преступников, покушающихся именно на банки (в отличие от, например, промышленных компаний, внутренняя информация которых мало кому интересна). Информация в банковских системах затрагивает интересы большого количества людей и организаций - клиентов банка. Как правило, она конфиденциальна, и банк несет ответственность за обеспечение требуемой степени секретности перед своими клиентами. Естественно, клиенты вправе ожидать, что банк должен заботиться об их интересах, в противном случае он рискует своей репутацией со всеми вытекающими отсюда последствиями.

Конкурентоспособность банка зависит от того, насколько клиенту удобно работать с банком, а также насколько широк спектр предоставляемых услуг, включая услуги, связанные с удаленным доступом. Поэтому клиент должен иметь возможность быстро и без утомительных процедур распоряжаться своими деньгами. Но такая легкость доступа к деньгам повышает вероятность преступного проникновения в банковские системы.

Информационная безопасность банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, поскольку банк несет ответственность не только за свои средства, но и за деньги клиентов. Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации.

К сожалению, в наши дни, в связи с высоким развитием технологий, даже предельно жесткие организационные меры по упорядочению работы с конфиденциальной информацией не защитят от ее утечки по физическим каналам. Поэтому системный подход к защите информации требует, чтобы средства и действия, используемые банком для обеспечения информационной безопасности (организационные, физические и программно-технические), рассматривались как единый комплекс взаимосвязанных,

взаимодополняющих и взаимодействующих мер. Такой комплекс должен быть нацелен не только на защиту информации от несанкционированного доступа, но и на предотвращение случайного уничтожения, изменения или разглашения информации.

2 Основные проблемы и задачи обеспечения защиты информации в условиях применения компьютерной технологии ведения банковского делопроизводства

2.1 Основные проблемы и задачи

Современная (компьютерная) технология ведения банковского делопроизводства обладает неоспоримыми преимуществами, как то: быстрая (автоматизированная) реализация процессов и операций расчетов, документирования и иных; возможность компактного представления и хранения информации, ее дублирования, контроля, пополнения, аварийного уничтожения и т.д. Вместе с тем, злоумышленники (обладающие достаточными знаниями в вопросах автоматизированного банковского делопроизводства, а иная - неавтоматизированная технология в современных условиях и немыслима) при определенной стратегии действий могут снять из компьютерных баз данных несанкционированным образом жизненно важную для деятельности и безопасности банка информацию. Это в последующем может привести к грамотно организованным преступным акциям по ограблению или дискредитации банка.

По данным экспертов, такой род преступных действий против банков получает все более широкое развитие. Следовательно, обеспечение безопасности средств вычислительной техники и информации, хранящейся в них, является делом не менее актуальным, чем все остальные задачи обеспечения безопасности, ибо, по крайней мере умозрительно, хищение информации и проведение незаконных банковских операций через АСОИ, потенциальному преступнику представляются менее опасными. Объективно он прав, т. к. если система защиты АСОИ имеет пробелы или построена на малоэффективных аппаратно-программных средствах, то обнаружение факта осуществления НСД или НСК практически маловероятно.

Потеря или даже относительно небольшая утечка информации может привести к тяжелым последствиям. Так, например, разорились практически все небольшие фирмы, вычислительные системы которых находились на нижнем этаже одного из здания делового центра Нью-Йорка, затопленного во время наводнения. Сумели выжить только крупные корпорации, базы данных которых были продублированы. У некоторых из них базы данных находятся в разных городах США. По некоторым данным, утечка 20% коммерческой информации в 60% приводит к банкротству фирмы.

Большинство ЭВМ, имеющихся в банке, как правило, объединены в локальные вычислительные сети (ЛВС), т. е. соединены между собой линиями связи и могут передавать друг другу хранящуюся в их памяти информацию, включая и результаты расчетных операций.

Область деятельности по обеспечению безопасности АСОИ, баз данных и ЛВС также многогранна, как и все иные виды деятельности, связанные с обеспечением безопасности. Именно поэтому разработчики системной концепции максимально широко рассматривают основные требования по организации защиты ПЭВМ, ЛВС, программного обеспечения, баз данных и в целом АСОИ, связуя их с требованиями иных блоков задач. В дальнейшем мы рассмотрим соответствующие рекомендации, методы и способы обеспечения этой защиты, включая требования и рекомендации по размещению ПЭВМ в здании, по электропитанию, заземлению, по защите ЭВМ от воздействия через вспомогательные технические средства (т. е. средства, имеющие выход за пределы штатно контролируемой зоны), монтажу и прокладке кабелей, по применению систем активного зашумления, экранированию и т. д. Системное понимание всего этого поможет правильно организовать разработку проекта защиты АСОИ.

В проблеме безопасности информации рассматриваются преднамеренная и непреднамеренная деятельность человека (в том числе ошибки программного обеспечения), неисправности технических средств, стихийные бедствия, которые могут привести к утечке, модификации или уничтожению информации.

Задача обеспечения безопасности информации, обрабатываемой в АСОИ, компьютерных сетях или в отдельно взятых ПЭВМ, сквозь призму системной концепции защиты требует для своего решения учета множества факторов: от архитектурных особенностей здания, в котором размещаются средства вычислительной техники, местоположения здания и т. д. (т. е. с этапа проектирования), до взаимодействия пользователей, программистов, сотрудников службы технического обслуживания и ремонта, администрации, службы безопасности (охраны) на этапе эксплуатации. Многообразие и актуальность вопросов обеспечения информационной безопасности породили обширную область исследований и разработок технических и программных методов и способов защиты.

Постоянное увеличение объема знаний в этой области, появление новых более эффективных программных, аппаратных средств защиты информации приводят к необходимости систематического учета состояния этой области и внесения соответствующих корректив в способы организации работы в АСОИ, а также в технологию обработки информации.

По мнению наиболее известных специалистов, проблема безопасности ЭВМ представляет собой как управленческую, так и техническую задачу и может оказывать значительное влияние на прогресс или регресс в использовании компьютерной техники и компьютерных технологий.

В настоящее время все больший размах в мире приобретает информационное пиратство: несанкционированное копирование программных продуктов и данных, компьютерные диверсии (вирусы, компьютерные «бомбы», «троянские кони» и т. п.), финансовые преступления с использованием вычислительной техники и т. д. В этой связи весьма актуальной становится задача обеспечения компьютерной безопасности.

Среди множества приемов и методов защиты информации (организационные, технические, программные, программно-аппаратные, криптографические и т. д.) особо следует выделить именно программные в силу следующих факторов:

простота тиражирования программных систем защиты на объекты заказчика и разработчика;

простота технологии применения;

применение программных методов не требует привлечения производства и возможно в самые короткие сроки, при этом позволяя получить достаточный уровень защищенности данных.

Качественное и своевременное обеспечение компьютерной безопасности программными методами во многом определяется уровнем развития теории программирования и умением разработчиков применять специальные приемы. При этом, естественно, что совершенствование систем защиты влечет за собой совершенствование приемов «взлома», защитных механизмов и эта тенденция делает необходимым постоянное ведение научно-исследовательских работ в области системного программирования.

2.2 Проблема нарушений функционирования АСОИБ

Не будет преувеличением сказать, что проблема умышленных нарушений функционирования АСОИБ различного назначения в настоящее время является одной из самых актуальных. Наиболее справедливо это утверждение для стран с сильно развитой информационной инфраструктурой, о чем убедительно свидетельствуют приводимые ниже цифры.

Известно, что в 1992 году ущерб от компьютерных преступлений составил $555 млн., 930 лет рабочего времени и 15.3 года машинного времени. По другим данным ущерб финансовых организаций составляет от $173 млн. до $41 млрд. в год.

Из данного примера, можно сделать вывод, что системы обработки и защиты информации отражают традиционный подход к вычислительной сети как к потенциально ненадежной среде передачи данных. Существует несколько основных способов

обеспечения безопасности программно-технической среды, реализуемых различными методами:

Рисунок 2 - Способы защиты информации в банках

Идентификация (аутентификация) и авторизация при помощи паролей.

Создание профилей пользователей. На каждом из узлов создается база данных пользователей, их паролей и профилей доступа к локальным ресурсам вычислительной системы.

Создание профилей процессов. Задачу аутентификации выполняет независимый (third-party) сервер, который содержит пароли, как для пользователей, так и для конечных серверов (в случае группы серверов, базу данных паролей также содержит только один (master) сервер аутентификации; остальные - лишь периодически обновляемые копии). Таким образом, использование сетевых услуг требует двух паролей (хотя пользователь должен знать только один - второй предоставляется ему сервером «прозрачным» образом). Очевидно, что сервер становится узким местом всей системы, а его взлом может нарушить безопасность всей вычислительной сети.

Инкапсуляция передаваемой информации в специальных протоколах обмена. Использование подобных методов в коммуникациях основано на алгоритмах шифрования с открытым ключом. На этапе инициализации происходит создание пары ключей - открытого и закрытого, имеющегося только у того, кто публикует открытый ключ. Суть алгоритмов шифрования с открытым ключом заключается в том, что операции шифрования и дешифрования производятся разными ключами (открытым и закрытым соответственно).

Ограничение информационных потоков. Это известные технические приемы, позволяющие разделить локальную сеть на связанные подсети и осуществлять контроль и ограничение передачи информации между этими подсетями.

Firewalls (брандмауэры). Метод подразумевает создание между локальной сетью банка и другими сетями специальных промежуточных серверов, которые инспектируют, анализируют и фильтруют весь проходящий через них поток данных (трафик сетевого/транспортного уровней). Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода - это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая закрытую локальную сеть практически невидимой.

Proxy-servers. При данном методе вводятся жесткие ограничения на правила передачи информации в сети: весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью - попросту отсутствует маршрутизация как таковая, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными в принципе. Очевидно также, что этот метод не дает достаточной защиты против атак на более высоких уровнях, например на уровне программного приложения.

Создание виртуальных частных сетей (VPN) позволяет эффективно обеспечивать конфиденциальность информации, ее защиту от прослушивания или помех при передаче данных. Они позволяют установить конфиденциальную защищенную связь в открытой сети, которой обычно является интернет, и расширять границы корпоративных сетей до удаленных офисов, мобильных пользователей, домашних пользователей и партнеров по бизнесу. Технология шифрования устраняет возможность перехвата сообщений, передаваемых по виртуальной частной сети, или их прочтения лицами, отличными от авторизованных получателей, за счет применения передовых математических алгоритмов шифрования сообщений и приложений к ним. Концентраторы серии Cisco VPN 3000 многими признаются лучшим в своей категории решением удаленного доступа по виртуальным частным сетям. Концентраторы Cisco VPN 3000, обладающие самыми передовыми возможностями с высокой надежностью и уникальной, целенаправленной архитектурой. Позволяют корпорациям создавать инфраструктуры высокопроизводительных, наращиваемых и мощных виртуальных частных сетей для поддержки ответственных приложений удаленного доступа. Идеальным орудием создания виртуальных частных сетей от одного сетевого объекта к другому служат

маршрутизаторы Cisco, оптимизированные для построения виртуальных частных сетей, к которым относятся маршрутизаторы Cisco 800, 1700, 2600, 3600, 7100 и 7200.

Системы обнаружения вторжений и сканеры уязвимости создают дополнительный уровень сетевой безопасности. Хотя межсетевые экраны пропускают или задерживают трафик в зависимости от источника, точки назначения, порта или прочих критериев, они фактически не анализируют трафик на атаки и не ведут поиск уязвимых мест в системе. Кроме того, межсетевые экраны обычно не борются с внутренними угрозами, исходящими от "своих". Система обнаружения вторжений CiscoIntrusionDetectionSystem (IDS) может защитить сеть по периметру, сети взаимодействия с бизнес-партнерами и все более уязвимые внутренние сети в режиме реального времени. Система использует агенты, представляющие собой высокопроизводительные сетевые устройства, для анализа отдельных пакетов с целью обнаружения подозрительной активности. Если в потоке данных в сети проявляется несанкционированная активность или сетевая атака, агенты могут обнаружить нарушение в реальном времени, послать сигналы тревоги администратору и заблокировать доступ нарушителя в сеть. Помимо сетевых средств обнаружения вторжений компания Cisco также предлагает серверные системы обнаружения вторжений, обеспечивающие эффективную защиту конкретных серверов в сети пользователя, в первую очередь серверов WEB и электронной коммерции. CiscoSecureScanner представляет собой программный сканер промышленного уровня, позволяющий администратору выявлять и устранять уязвимости в сетевой безопасности прежде, чем их найдут хакеры.

По мере роста и усложнения сетей первостепенное значение приобретает требование наличия централизованных средств управления политикой безопасности, которые могли бы управлять элементами безопасности. Интеллектуальные средства, которые могут обозначать состояние политики безопасности, управлять ею и выполнять аудит, повышают практичность и эффективность решений в области сетевой безопасности. Решения Cisco в этой области предполагают стратегический подход к управлению безопасностью. CiscoSecurePolicyManager (CSPM) поддерживает элементы безопасности Cisco в корпоративных сетях, обеспечивая комплексную и последовательную реализацию политики безопасности. С помощью CSPM клиенты могут определять соответствующую политику безопасности, внедрять ее в действие и проверять принципы безопасности в работе сотен межсетевых экранов CiscoSecure PIX и Cisco IOS FirewallFeatureSet и агентов IDS. CSPM также поддерживает стандарт IPsec для построения виртуальных частных сетей VPN. Кроме того, CSPM является составной

частью широко распространенной корпоративной системы управления CiscoWorks2000/VMS.

Суммируя приведенные способы, можно сказать, что разработка информационных систем требует параллельной разработки технологий передачи и защиты информации. Эти технологии должны обеспечивать защиту передаваемой информации, делая сеть «надежной», хотя надежность на современном этапе понимается как надежность не на физическом уровне, а скорее на логическом (информационном уровне).

Существует также ряд дополнительных мероприятий, реализующих следующие принципы:

Мониторинг процессов. Метод мониторинга процессов заключается в создании специального расширения системы, которое бы постоянно осуществляло некоторые типы проверок. Очевидно, что некоторая система становится внешне уязвимой только в том случае, когда она предоставляет возможность доступа извне к своим информационным ресурсам. При создании средств такого доступа (серверных процессов), как правило, имеется достаточное количество априорной информации, относящейся к поведению клиентских процессов. К сожалению, в большинстве случаев эта информация попросту игнорируется. После аутентификации внешнего процесса в системе он в течение всего своего жизненного цикла считается авторизованным для доступа к некоторому количеству информационных ресурсов без каких-либо дополнительных проверок.

Хотя указать все правила поведения внешнего процесса в большинстве случаев не представляется возможным, вполне реально определить их через отрицание или, иначе говоря, указать, что внешний процесс не может делать ни при каких условиях. На основании этих проверок можно осуществлять мониторинг опасных или подозрительных событий. Например, на приведенном рисунке показаны элементы мониторинга и выявленные события: DOS-атака; ошибка набора пароля пользователем; перегрузки в канале связи.

Дублирование технологий передачи. Существует риск взлома и компрометации любой технологии передачи информации, как в силу ее внутренних недостатков, так и вследствие воздействия извне. Защита от подобной ситуации заключается в параллельном применении нескольких отличных друг от друга технологий передачи. Очевидно, что дублирование приведет к резкому увеличению сетевого трафика. Тем не менее, такой способ может быть эффективным, когда стоимость рисков от возможных потерь оказывается выше накладных расходов по дублированию.

Децентрализация. Во многих случаях использование стандартизованных технологий обмена информацией вызвано не стремлением к стандартизации, а

недостаточной вычислительной мощностью систем, обеспечивающих процедуры связи. Реализацией децентрализованного подхода может считаться и широко распространенная в сети Internet практика «зеркал». Создание нескольких идентичных копий ресурсов может быть полезным в системах реального времени, даже кратковременный сбой которых может иметь достаточно серьезные последствия.

Заключение

Как мы уже увидели из всего вышеизложенного в данной работе, банки играют большую роль в жизни нашего современного общества. Сейчас банки уже полностью перешли к компьютерной обработке информации, что значительно повысило производительность труда, ускорило расчеты и привело к появлению новых услуг. Однако компьютерные системы, без которых в настоящее время не может обойтись ни один банк, являются также источником совершенно новых угроз, неизвестных ранее. Большинство из них обусловлены новыми информационными технологиями и не являются специфическими исключительно для банков.

Существуют, однако, два аспекта, выделяющих банки из круга остальных коммерческих систем:

1. Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т. д.

2. Она затрагивает интересы большого количества организаций и отдельных лиц.

Поэтому информационная безопасность банка -- критически важное условие его существования.

В силу этих обстоятельств, к банковским системам предъявляются повышенные требования относительно безопасности хранения и обработки информации. Отечественные банки также не смогут избежать участи тотальной автоматизации по следующим причинам:

- усиления конкуренции между банками;

- необходимости сокращения времени на производство расчетов;

- необходимости улучшать сервис.

Сфера информационной безопасности -- наиболее динамичная область развития индустрии безопасности в целом. Если обеспечение физической безопасности имеет давнюю традицию и устоявшиеся подходы, то информационная безопасность постоянно

требует новых решений, т. к. компьютерные и телекоммуникационные технологии постоянно обновляются, на компьютерные системы возлагается все большая ответственность.

Итак, автоматизация и компьютеризация банковской деятельности (и денежного обращения в целом) продолжает возрастать. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Можно прогнозировать дальнейшее снижение оборота наличных денег и постепенный переход на безналичные расчеты с использованием пластиковых карт, сети Интернет и удаленных терминалов управления счетом юридических лиц.

Список использованной литературы

1. Полетаева К.А. Обеспечение информационной безопасности банковской системы // Скиф. 2018. №4 (20). URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-bankovskoy-sistemy (дата обращения: 31.05.2023).

2. Мордвинова, Е. А. Информационная безопасность банковских продуктов и услуг в России / Е. А. Мордвинова. — Текст : непосредственный // Молодой ученый. — 2021. — № 21 (363). — С. 239-241. — URL: https://moluch.ru/archive/363/81377/ (дата обращения:31.05.2023).

3. Беспалова, И. В. Необходимость усиления информационной безопасности банковского сектора / И. В. Беспалова // Проблемы и перспективы развития кооперации и интеграции в современной экономике: Сборник статей I Международной научно-практической конференции, Энгельс, 13–14 декабря 2018 года. — Энгельс: ООО «Центр социальных агроинноваций СГАУ», 2018. — С. 34–38.

4. Манаенкова, Е. С. Направления развития банковских продуктов и услуг в России / Е. С. Манаенкова // Российская экономика: взгляд в будущее: Материалы VII Международной научно-практической конференции, Тамбов, 26 февраля 2021 года / Отв. редактор Я. Ю. Радюкова. — Тамбов: Тамбовский государственный университет имени Г. Р. Державина, 2021. — С. 217–232.

5. Сипратов, Р. О. Оценка рисков информационной безопасности кредитно-финансовой сферы и пути их снижения / Р. О. Сипратов // Актуальные вопросы современной экономики. — 2021. — № 2. — С. 369–375

6. Голубитченко, М. А. Особенности информационной безопасности в кредитно-финансовой сфере / М. А. Голубитченко, Е. П. Беренвальд, Е. Е. Парасюк. — Текст :

непосредственный // Молодой ученый. — 2021. — № 52 (394). — С. 9-13. — URL: https://moluch.ru/archive/394/87219/ (дата обращения: 31.05.2023).

7. ГОСТ Р 57580.1–2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер // Федеральное агентство по техническому регулированию и метрологии. Официальное издание. М.: Стандартинформ, 2020.

8. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) // СПС «КонсультантПлюс».

9. *Внуков, А. А.* Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269 (дата обращения: 31.05.2023).

10. Горян Элла Владимировна Роль финансового регулятора в обеспечении кибербезопасности в России и Сингапуре: сравнительно-правовой аспект // Территория новых возможностей. 2019. №2. URL: https://cyberleninka.ru/article/n/rol-finansovogo-regulyatora-v-obespechenii-kiberbezopasnosti-v-rossii-i-singapure-sravnitelno-pravovoy-aspekt (дата обращения: 31.05.2023).

11. Шамсутдинов Ринат Рустемович Обеспечение безопасности информационных технологий в банковских организациях Российской Федерации // Colloquium-journal. 2019. №3-1 (27). URL: https://cyberleninka.ru/article/n/obespechenie-bezopasnosti-informatsionnyh-tehnologiy-v-bankovskih-organizatsiyah-rossiyskoy-federatsii (дата обращения: 31.05.2023).

12. Болурова М.И., Салпагарова М.У., Шакова Ф.М. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ // Вестник науки. 2019. №10 (19). URL: https://cyberleninka.ru/article/n/problemy-obespecheniya-informatsionnoy-bezopasnosti-v-bankovskom-sektore (дата обращения: 31.05.2023).