«УТВЕРЖДЕНО»
Постановлением Правления
Национального банка Таджикистана
за №___ от «___» _____ 2021 г.

Минимальные требования к программно-техническому обеспечению кредитных финансовых организаций

Минимальные требования к программному и техническому обеспечению кредитных финансовых организаций (далее - Требования) разработаны в соответствии с частью 5 статьи 42 Закона Республики Таджикистан «О Национальном банке Таджикистана» с целью обеспечения необходимого уровня информационной безопасности в банковской системе Республики Таджикистан, достижения необходимого уровня защиты от реальных рисков кибератак и минимизации ущерба, причиненного в результате нарушения информационных систем или информационной безопасности, устанавливает минимальные требования к программному и техническому обеспечению кредитных финансовых организаций.

ГЛАВА 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1. Основные понятия используемые в документе:

- BankNet - защищенная корпоративная сеть, используемая для доступа кредитной финансовой организации к рабочим системам Национального банка Таджикистана;
- Advanced Encryption Standard (AES) - это алгоритм симметричного блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительства США;
- Demilitarized Zone (DMZ)- часть сети, которая включает в себя общедоступные службы и отделяет их от частных служб;
- Global Positioning System (GPS) - спутниковая навигационная система, которая измеряет расстояние и время и определяет местоположение в международной системе координат WGS 84;
- Intrusion Detection System (IDS) - программное или аппаратное обеспечение, предназначенное для обнаружения несанкционированного доступа к компьютерной системе или сети;

- Intrusion Prevention System (IPS) - программное или аппаратное обеспечение, предназначенное для предотвращения несанкционированного доступа к компьютерной системе или сети;
- International Organization for Standardization (ISO) - международная организация, разрабатывающая стандарты;
- Local Area Network (LAN) - компьютерная сеть, соединяющая компьютеры, расположенные на небольшой территории или недалеко друг от друга;
- National Institute of Standards and Technology (NIST) - Национальный институт стандартов и технологий;
- Open Database Connectivity (ODBC) - программный интерфейс для доступа к базам данных;
POS-терминал - электронное программно- техническое оборудование для приема платежных карт к оплате;
- registered Jack (RJ45) - зарегистрированный разъем с серийным номером 45;
- structured Query Language (SQL) - декларативный язык программирования, используемый для создания, изменения и управления данными в реляционной базе данных;
- коммутатор - сетевое устройство, используемое для соединения нескольких узлов компьютерной сети в одной или нескольких частях сети;
- цифровой сертификат - электронный документ, выданный органом по сертификации и подтверждающий право собственности на открытый ключ или другой атрибут;
- файрвол - устройство или приложение, предназначенное для фильтрации (разрешения или запрета) передачи данных по сети. Файрвол работает в соответствии с набором правил, предназначенных для защиты сетей от неофициального доступа;
- автоматизированная банковская система (АБС) - автоматизированная банковская система - комплекс программного и технического обеспечения, предназначенный для автоматизации банковских бизнес-процессов;
- база данных (БД) - это организованная структура, предназначенная для хранения, изменения и обработки взаимосвязанных данных;
- система управления базами данных (СУБД) - набор программного обеспечения, предназначенный для построения новой структуры базы

данных, наполнения ее данными, внесения изменений и отображения данных;
- интеграция информационных систем (ИИС) - это процесс установления связи между информационными системами кредитной финансовой организации, который предназначен для достижения единой информационной среды и организации обеспечения ее бизнес – процессов;
- электронный кошелек - программа или программный комплекс, позволяющий хранить электронные деньги и совершать с ними безналичные операции;
- резервное копирование данных - процесс создания резервной копии данных на оборудовании передачи данных, предназначенный для восстановления данных в старом или новом месте в случае повреждения или потери данных;
- восстановление данных - процесс восстановления данных в старом месте;
- пароль - условное слово или набор символов, используемых для идентификации физического лица или обязательства;
- компьютерный вирус - разновидность вредоносного ПО, которое проникает в код других программ, в области системной памяти и загрузочные секторы и распространяет свои копии по различным каналам связи;
- антивирусные программы - специальные компьютерные программы, предназначенные для обнаружения компьютерных вирусов;
- аутентификация - это процесс проверки подлинности чего-либо / человека. Например, процесс аутентификации путем сравнения пароля, введенного пользователем, с паролем, введенным в информационной системе;
- множественная аутентификация - широкая аутентификация, метод контроля доступа к компьютеру, в котором пользователь должен предоставить более одного доказательства механизма аутентификации для доступа к данным;
- двоичная аутентификация - вид многоуровневой аутентификации, метод идентификации пользователя путем запроса аутентификационных данных различных типов;
- авторизация - предоставление права определенному лицу или группе лиц на выполнение определенных операций, а также процесс проверки прав при выполнении этих операций.

2. Данные требования помогают достигнуть следующих целей:

- создание инфраструктуры ИТ-безопасности в кредитной финансовой организации и создание совершенно надежной среды для информационных и коммуникационных технологий;
- разработать политику безопасности в соответствии с международными стандартами безопасности и передовой практикой;
- укрепление нормативной правовой базы для обеспечения безопасной среды в кредитной финансовой организации;
- повышение уровня защиты и устойчивости кредитной финансовой организации при проектировании, разработке и внедрении информационных ресурсов;
- интегрировать продукты и услуги ИКТ путем создания инфраструктуры для управления этими продуктами и услугами;
- оценка рисков деятельности ИКТ;
- повышение осведомленности и обеспечение безопасности человеческих ресурсов.

3. Кредитных финансовых организации должны обеспечивать выполнение следующих мер для защиты информации :

- уделить особое внимание информационной безопасности и принять необходимые меры для защиты информации и управления информационными системами.
- постоянно улучшать свое программное обеспечение и приводить его в соответствие с общепринятыми стандартами.
- при управлении операционными рисками Кредитных финансовых организации должны учитывать и документировать информационные риски финансовых операций, а также меры по их снижению.
- учитывать стабильность и безопасность информационных процессов, которые могут повлиять на непрерывность деятельности кредитных финансовых организаций, их клиентов и поставщиков услуг.
- понять и правильно оценить угрозы информационной безопасности и возможности существующих систем безопасности по снижению рисков.

- в случае участия в обработке, хранении или передаче информации, связанной с банковскими платежными картами, электронными кошельками, банкоматами или электронными терминалами (POS-терминалами) необходимо иметь соответствующий сертификат.
- методологии управления рисками для обеспечения устойчивости, информации и непрерывности бизнеса должны соответствовать международным стандартам NIST и ISO.

ГЛАВА 2. СТРАТЕГИЯ И ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4. Стратегия информационной безопасности должна быть одобрена руководством кредитной финансовой организации. Эта стратегия должна охватывать как минимум следующие области:

1) среда киберугроз и возможное влияние на деятельность кредитной финансовой организации;
2) подходы к управлению рисками информационной безопасности, а также к выявлению и мониторингу киберугроз и угроз информационной безопасности;
3) принципы реализации мер кибербезопасности и информации.

5. законодательство в области стратегии информационной безопасности должно соответствовать нормативным правовым актам Республики Таджикистан, а также международным стандартам информационной безопасности (ISO27001).
6. Стратегию следует пересматривать не реже одного раза в два года, независимо от того, какие обновления требуются в течение этого периода.
7. Внутренние нормативные акты, касающиеся требований информационной безопасности кредитной финансовой организации, могут включать, но не ограничиваются, положениями настоящего закона.
8. Внутренними нормативными актами должны определяться политика и стратегия кредитной финансовой организации в области информационной безопасности в соответствии с этими требованиями. Также внутренние внутренние нормативные акты должны соответствовать всем процессам контроля и методам достижения целей кредитной финансовой организации в области информационной безопасности.

9. Во внутренних нормативных актах должны отражаться следующие аспекты:

- основные цели и потребность в информационной безопасности;
- ответственность сотрудников за кибербезопасность и информацию;
- подробное описание необходимых мер контроля и эксплуатации, а также систем мониторинга и реагирования;
- повышение осведомленности сотрудников, деловых партнеров, поставщиков, поставщиков услуг и клиентов;
- сбор и обмен информацией между сотрудниками и другими учреждениями.

10. Необходимо разработать и регулярно обновлять конкретные политики для реализации мер безопасности на основе киберполитики и информационной безопасности.
11. На основе современных отраслевых инноваций в области информационной безопасности должна быть установлена конкретная процедура, охватывающая все вопросы кибербезопасности и информации.
12. Процедура должна включать подробную информацию, включая каждый этап, процесс и инфраструктуру, относящиеся к финансовым операциям, безопасности, резервному копированию данных, надежности системы, восстановлению данных и управлению данными.
13. Процессы следует пересматривать ежегодно или, при необходимости, после изменений в соответствующей деловой или технологической среде.

ГЛАВА 3. ПЕРЕЧЕНЬ АКТИВОВ ИКТ

14. Кредитным финансовым организациям следует составить список всех активов в области информационных и коммуникационных технологий.
15. Этот реестр должен содержать следующую информацию об активах:

- материальные и нематериальные институциональные информационные активы;
- материальные и нематериальные информационные активы, которые не находятся в помещении кредитной финансовой организации, но находятся под её ответственностью;

- информационные активы, которые выходят за рамки ответственности кредитной финансовой организации, но отсутствие этих активов или их недееспособность может повлиять на организацию.

16. Назначить ответственное лицо по каждому активу за счет сотрудников соответствующих структурных подразделений кредитной финансовой организации со следующими полномочиями и обязанностями:

- использование активов;
- обеспечение целостности актива и инструкции по его использованию в случае инцидентов, связанных с информационной безопасностью;
- копирование и обеспечение восстановления активов после аварии;
- контроль активов информационных технологий, идентификация ответственных лиц и политик доступа к этим активам.

17. Все сотрудники должны соответствовать принятым требованиям по использованию актива, и их соответствие должно быть задокументировано.

18. Каждый информационный актив следует разделить на следующие группы:

- значение или стоимость активов для кредитной финансовой организации;
- чувствительность к кибербезопасности и информационной безопасности, а также к правовым аспектам;
- размер ущерба в случае повреждения, подделки или незаконного присвоения информационных активов кредитной финансовой организации финансовому учреждению.

ГЛАВА 4. ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ И АРХИТЕКТУРЕ ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

19. Принципы работы инфраструктуры информационных и коммуникационных технологий должны соответствовать требованиям информационной безопасности кредитной финансовой организации.

20. Инфраструктура информационных и коммуникационных технологий должна соответствовать уровню рисков безопасности, чувствительности информации, ожидаемому уровню потерь и требованиям законодательства.

21. Кредитная финансовая организация должна применять необходимые методы и меры для предотвращения, обнаружения, исправления и документирования нарушений своей IT-системы.
22. Внутренняя коммуникационная сеть кредитной финансовой организации должна распределяться в соответствии с критериями, связанными с организационной структурой, деятельностью и чувствителностью информации.
23. Кредитных финансовых организации должны запретить использование устройств передачи данных сотрудниками без разрешения.
24. Необходимо установить антивирусное программное обеспечение, чтобы предотвратить проникновение вредоносных программ в сети, системы, серверы и рабочие места.
25. Файлы, содержащие конфиденциальную информацию, должны быть зашифрованы.
26. Кредитной финансовой организации следует проводить регулярный мониторинг информационных и коммуникационных технологий с целью выявления подозрительных действий или нарушений политики безопасности.

ГЛАВА 5. ТРЕБОВАНИЯ К ЛОКАЛЬНОЙ СЕТИ И СЕТЕВОМУ ОБОРУДОВАНИЮ

27. Внутренняя сеть кредитной финансовой организации должна соответствовать стандартам эффективности, надежности и безопасности.
28. Размер внутренней сети может быть ограничен двумя компьютерами и более.
29. Кабельная система должна соответствовать требованиям ISO / IEC 11801.
30. Для подключения к внутренней сети на каждом рабочем месте должно быть хотя бы одно гнездо RJ-45.
31. Все разъемы RJ-45 на рабочих местах и коммутаторы должны быть промаркированы типографским или принтерным способом.
32. При прокладке сетевых кабелей необходимо учитывать следующие требования:
- кабели следует прокладывать за подвесными потолками, стенами из гипсокартона, в специальных местах или кабельных каналах.

- кабели необходимо закрепить по всей длине специальными материалами (коробками).
- оборудование и схемы должны быть обеспечены двойными мерами предосторожности.
- после монтажа и прокладки кабеля не следует нарушать эстетический вид здания.

33. Сетевое оборудование должно работать круглосуточно (24/7). Время профилактического обслуживания не учитывается.

34. Количество портов сетевого оборудования (или их комбинация) должно охватывать работу всех (100%) рабочих мест и иметь не менее 20% запасных частей.

35. Роутер должен иметь функцию межсетевого экрана и возможность назначать списки доступа для сетевой интеграции.

36. Все неиспользуемые сетевые порты необходимо отключить вручную или с помощью программы управления доступом к сети.

37. Кредитных финансовых организации должны иметь резервную копию конфигурации сетевого оборудования и элементов защиты информации в зашифрованном виде.

38. Внутренняя сеть должна быть защищена системой безопасности, которая контролирует скорость входящей и исходящей сети на основе установленных правил безопасности (например, межсетевого экрана).

39. Внутренняя сеть должна быть физически или мысленно отделена от внешней сети. Кредитная финансовая организация должна наложить строгие ограничения на использование файрволов (программного и / или аппаратного) между внутренними и внешними сетями (сетями Banknet, интернет-провайдерами, клиентами и поставщиками услуг).

40. Кроме того, Кредитных финансовых организации должны принять такие меры, как зона демилитаризации (DMZ), механизмы передачи данных, фильтрация и сегментация информации.

41. Кредитных финансовых организации должны установить специальное сетевое оборудование для защиты от атак. Это оборудование должно быть предназначено для предотвращения атак, сетевого наблюдения и системы от злонамеренных действий или нарушений политик безопасности внутренними и внешними злоумышленниками (включая IDS / IPS).

ГЛАВА 6. ТРЕБОВАНИЯ ДЛЯ УДАЛЁННОГО ДОСТУПА

42. Для удаленного доступа к корпоративной сети необходимо определить высокую степень идентификации и аутентификации
43. Все компоненты оборудования, которые имеют удаленный доступ к сети кредитных финансовых организаций, должны подписываться сертификатом цифровой подписи для аутентификации.
44. Кредитных финансовых организации должны предоставлять удаленный доступ к сети и ключевым системам только при необходимости. Доступ в таких случаях должен предоставляться в определенное время в соответствии с должностными обязанностями заявителя.
45. В случае удаленного доступа должно обеспечиваться соединение и безопасное шифрование.
46. Кредитным финансовым организациям необходимо использовать систему, к которой нет непосредственного удаленного доступа
47. Доступ должен осуществляться через защищенный сервер, который обеспечивает шифрование канала связи, управление паролями и контроль аудита.

ГЛАВА 7. ТРЕБОВАНИЯ ДЛЯ ДОСТУПА К ИНТЕРНЕТ

48. Доступ сотрудников к Интернету должен предоставляться непосредственно руководством кредитной финансовой организации на основании оценки рисков и принятия соответствующих мер контроля.
49. Сотрудник, перед доступом к сети Интернету, должен подписать документ, подтверждающий осведомленность о том, что разрешено и запрещено. В документе должно быть указано, что все действия пользователя контролируются. В этом документе также должны быть подробно описаны права и обязанности сотрудника при использовании интернет-услуг.
50. Сотрудник должен иметь доступ к Интернету с определенного рабочего места при соблюдении следующих условий:
1) рабочее место должно быть отделено от локальной сети на логическом или физическом уровне и не должно содержать конфиденциальную информацию или бизнес - программу кредитной организации (в том числе АБС).
2) подключение к Интернету должно осуществляться через отдельный прокси-сервер. Прокси-сервер должен постоянно быть защищенным и контролироваться.

51. На прокси-сервере и на рабочих станциях, подключенных к сети интернет, должны быть внедрены нижеследующие меры предосторожности:

- фильтрация контента и спама;
- предотвращение использования вредоносных ссылок;
- системы обнаружения вторжений (IDS);
- межсетевые экраны (файрволы);
- антивирусное программное обеспечение с актуализацией антивирусных баз;
- наличие черного списка сайтов;
- журнал аудита, документирующий все действия пользователя.

52. Необходимо проводить тесты на отказоустойчивость и проникновение для серверов, коммуникационного оборудования, подключенных к Интернету, включая почтовую инфраструктуру, не реже одного раза в квартал.

ГЛАВА 8. ТРЕБОВАНИЯ К ИСПОЛЬЗОВАНИЮ КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТЫ

53. Кредитная финансовая организация подготовит процедуры, детализирующие разрешенные и запрещенные действия в отношении электронной почты.

54. Сотрудник финансовой организации, которому разрешено использовать корпоративную электронную почту, должен подписать документ, подтверждающий осведомленность о разрешенных и запрещенных действиях, включая тот факт, что действия электронной почты постоянно отслеживаются.

55. Все файлы вложения, которые могут нанести угрозу системе (расширения *.exe, *.bat, *.com) автоматически должны блокироваться почтовой системой. Список расширений файлов может быть дополнен.

56. При использовании корпоративной электронной почты сотруднику запрещается:

- отправлять/принимать электронные письма не служебного характера;
- отправлять электронные письма с вложениями, содержащими вирусы и/или прочие вредоносные программы;
- рассылки, имеющие характер спама – письма “счастья” и тому подобное;

- сотрудникам запрещается переходить по ссылкам и вводить свои пароли и/или логины на страницах, вызывающие сомнения.

57. Почтовые серверы и системы электронной почты должны быть защищены с использованием мер безопасности, включая, помимо прочего, следующих ограничений:

- фильтрация контента и спама;
- система для обнаружения, блокировки и сообщения о нарушениях данных;
- файерволы;
- антивирусные программы.

ГЛАВА 9. ТРЕБОВАНИЯ К ВЕБСАЙТАМ И ВЕБ-ПРИЛОЖЕНИЯМ

58. Веб-сайт и WEB-программы должны соответствовать следующим требованиям:

- на каждой странице сайта должна быть возможность перехода на главную страницу;
- наличие страницы «О нас» и полной информации о кредитной финансовой организации;
- наличие удобного способа связи между пользователем и кредитной финансовой организацией;
- наличие возможностей поиска на сайте;
- наличие соответствующего сообщения для страницы ошибки 404 (Error 404) и наличие ссылки на пустые страницы или страницы с пометкой «в процессе обработки»;
- использование понятного определения для ссылок. При необходимости предоставление ссылок на статьи из других источников;
- роли, процедуры и руководства по управлению контентом сайта должны быть задокументированы.

59. На сайте должен быть специальный сервис, позволяющий анализировать сайт и собирать информацию о действиях его пользователей.

60. Сайт должен иметь как минимум контент, опубликованный на двух языках (таджикском и английском).

ГЛАВА 10. ТРЕБОВАНИЯ К КОНТРОЛЮ ДОСТУПА И АУТЕНТИФИКАЦИИ

61. Субъект, запрашивающий доступ к системам ИКТ кредитной финансовой организации, должен пройти процедуру идентификации и аутентификации.

62. В дополнение, банки должны иметь специализированные системы для управления и контроля разрешения доступа. Доступ к системам ИКТ должен контролироваться и документироваться со стороны аудита.

63. Методы доступа к ИКТ-системам должны быть стандартными, включая идентификацию и аутентификацию:

- идентификатор пользователя и пароль;
- проверка прав доступа с использованием доступа к серверным операционным системам.

64. Необходимо использовать технологию, которая объединяет идентификацию и аутентификацию пользователя, конфиденциальность и достоверность его личных данных.

65. Необходимо установить критерии для механизма тайм-аута сеанса после определенного периода бездействия пользователя в системе. Максимальное время тайм-аута - одна минута.

66. Необходимо устанавливать часы работы и даты, когда доступ к ресурсам ИКТ разрешен. Это расписание должно распространяться для всех сотрудников. Исключения из данных правил могут быть применены к администраторам, техническим специалистам.

67. При переводе сотрудника в другое подразделение все старые разрешения должны аннулироваться, а новые должны выдаваться в соответствии с новой должностью.

68. Доступ к корпоративной сети кредитной финансовой организации должен предоставляться только после идентификации и аутентификации пользователя.

69. Для критически важных систем должны быть разработаны механизмы двухфакторной аутентификации (биометрическая/ смарт-карта/токен/OTP).

70. Пользователям не разрешается использовать общую учетную запись. Каждый пользователь системы должен быть уникальным и идентифицируемым.

71. Задачи пользователей должны соответствовать утвержденному графику задач и должностным обязанностям.

72. Должен быть определен список сотрудников, работающих более чем на одной должности.

73. Права доступа сотрудников должны быть соразмерны их обязанностям.

ГЛАВА 11. ТРЕБОВАНИЯ К ПОЛИТИКЕ ПАРОЛЕЙ И УПРАВЛЕНИЮ ПАРОЛЯМИ

74. Минимальная длина пароля должна составлять восемь символов или соответствовать действующим стандартам.
75. Все пароли должны быть сложными и уникальными и содержать хотя бы один символ из четырех следующих категорий:
- заглавная буква (A-Z)
- строчные буквы (a-z)
- цифра (0-9)
- специальные символы (~ `! @ # $% ^ & * () + = _- {} [] \ |:;" '? / <> ,.)
76. Необходимо использовать механизм для создания начального пароля и он должен быть случайным.
77. Начальный пароль должен предоставляться пользователю по отдельному каналу.
78. Пароль, выданный пользователю может быть аннулирован в одном из следующих случаев:
- первоначальный пароль не использовался в течение трех дней после его выдачи;
- по запросу пользователя или в случаях, когда администратор подозревает, что пароль используется третьим лицом;
- после нескольких неудачных попыток входа в систему, но не более пяти последовательных попыток;
- после шести месяцев неиспользования системы, для которой был назначен пароль.
79. Кредитная финансовая организация должна иметь специальные механизмы для управления паролями сотрудников. Эти механизмы предоставляются посредством реализации программного обеспечения, которое включает хранение, замену в случае потери и замену пароля системным администратором без знания пароля сотрудника.

ГЛАВА 12. ТРЕБОВАНИЯ К СЕРВЕРНОМУ ОБОРУДОВАНИЮ И РАБОЧИМ МЕСТАМ

80. Оборудование, требующее защиты, включает любые устройства, которые сохраняют электронную информацию или используются как

часть серверов, ноутбуков, информационных платформ, телефонных станций, роутеров.

81. Уровень защиты для данного оборудования определяется в соответствии со следующими критериями:

- влияние на бизнес с точки зрения конфиденциальности целостности и доступности информации, хранящейся на соответствующем оборудовании;
- с точки зрения физической потери или недоступности оборудования.

82. Замена или списание оборудования должно происходить с учетом соблюдения следующих условий:

- вся информация, включая файлы журналов, параметры и настройки систем должны быть удалены или искажены;
- при необходимости носители (жесткие диски серверов и компьютеров) должны быть изъяты и уничтожены физически;
- физическое уничтожение носителей или всего изношенного оборудования должно быть оформлено специальным актом.

ГЛАВА 13. ТРЕБОВАНИЯ К АВТОМАТИЧЕСКОЙ БАНКОВСКОЙ СИСТЕМЕ

83. Общие требования к платформе Автоматизированной Банковской Системы (АБС):

- наличие общепонятного интерфейса;
- обеспечение связи между формами и минимизация ввода данных вручную;
- построение платформы по принципу единого ввода данных;
- обеспечение защиты данных и разграничение данных по уровню доступа;
- наличие модуля согласования данных и уведомления пользователей;
- обеспечение целостности и единого подхода к продвижению нормативной и каталожной информации;
- возможность интеграции с внешними системами;
- наличие модуля отчетности и аналитического модуля;
- предоставление интеграции или модулей для управления взаимоотношениями с клиентами, электронной коммерции и маркетинга;
- разработка всех функциональных модулей одной компанией и наличие линии техподдержки 24 часа в сутки, 7 дней в неделю, 365 (366) дней в году;

- доступ ко всем функциональным модулям платформы для работы со структурами данных;
- обеспечение возможности всех функциональных модулей платформы самостоятельно поддерживать и развивать систему без необходимости обязательной внешней консультации.

84. Бизнес приложения АБС должны соответствовать следующим требованиям:
- иерархическая структура инфраструктур кредитной финансовой организации;
- центры затрат;
- регулирование плана счетов с учетом филиалов;
- возможность ведения работы с планом счетов.
- раздел разработки контрактов, в том числе, основная информация (товары, валюта, валюта может быть изменена),бизнес партнер, финансовые условия;
- раздел «Кредиты», в том числе, основная информация по кредитным договорам, процентные ставки, срок, валюта, комиссия, штраф, штрафы за нарушение контракта, условия оплаты и др.
- раздел «Депозиты», в том числе, регламенты на продукцию, условия, валюта, срок, процентные ставки, фонды;
- блок «Снабжение»;
- блок обработки платежей;
- блок работы с пластиковыми картами.

ГЛАВА 14. ТРЕБОВАНИЯ К БАЗАМ ДАННЫХ

85. База данных должна соответствовать следующим требованиям:
- реализация SQL в соответствии с ANSI 1992;
- поддержка стандарта Open Database Connectivity (для ODBC);
- наличие возможности контролировать целостность базы данных;
- в любое время информация, содержащаяся в базе данных, должна быть точной и актуальной;
- надежность и целостность базы данных не должны быть нарушены во время технической эксплуатации.

86. Система управления базой данных должна обеспечивать следующие функции:
- непосредственное управление информацией во внешней и оперативной памяти и обеспечение эффективного доступа к ней в процессе решения задач;

- целостность данных и управление транзакциями;
- ведение системного журнала изменений в БД для обеспечения восстановления БД после технического или программного сбоя;
- реализация поддержки языка описания данных и языка запросов;
- обеспечение безопасности данных;
- обеспечение параллельного доступа к данным нескольких пользователей.

ГЛАВА 15. ТРЕБОВАНИЕ К ДИСТАНЦИОННЫМ БАНКОВСКИМ УСЛУГАМ

87. Кредитная финансовая организация должна определить виды дистанционных банковских услуг, предоставляемых для своих клиентов.
88. Использование устройств, поддерживающих мобильные приложения, которые не поддерживают соответствующий уровень шифрования (таких как AES с длиной ключа не менее 128 бит и цифровой подписью) не допускается.
89. Пользователь / клиент должен дать согласие на использование услуг дистанционного банковского обслуживания кредитной финансовой организации. Запись этого соглашения должна храниться на компьютерах организации. Уведомление о получении согласия пользователя на использование приложения рассылается по сетям, например по SMS.
90. Приложение должно быть проверено на предмет его кибер и информационной безопасности до его передачи клиентам и результаты проверки должны быть оформлены специальным актом.
91. Приложение не должно запрашивать разрешения, кроме тех, которые необходимы для выполнения его функций.
92. Передача информации через приложение должна быть минимально необходимой для ее использования.
93. Приложение не должно хранить конфиденциальную информацию на мобильном устройстве. Данные должны храниться в зашифрованном виде с использованием механизмов устройства, когда это необходимо.
94. Хранение исторической информации, данных GPS или любой другой конфиденциальной информации не должно превышать промежуток времени, необходимый для работы приложения.

95. Конфиденциальная личная информация должна быть удалена после выхода из приложения.
96. Необходимо наличие механизмов идентификации и аутентификации для проверки личности пользователей приложения.
97. Информация, передаваемая в приложение или из приложения, должна быть зашифрована и иметь цифровую подпись в пределах возможностей устройств.
98. Приложение не должно иметь возможность использовать и / или передавать данные с устройства пользователя, которые не нужны для работы приложения.
99. Перед установкой программа должна обязательно напоминать пользователю об области доступа к устройству и его сервисам.

ГЛАВА 16. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ СОТРУДНИКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

100. Каждый сотрудник кредитной финансовой организации обязан:
- пройти курс обучения, необходимый для выполнения сотрудниками своих обязанностей, и иметь соответствующий документ подтверждающий это;
- пройти учебный курс по безопасности, конфиденциальности и защите информации, ознакомиться с документами в области защиты информации и подписать его;
- соблюдать конфиденциальность официальной информации;
- владеть информацией о разрешенных и запрещенных действиях и нести персональную ответственность за нарушение требований защиты информации;
- обладать достаточными знаниями в области информационной безопасности и кибербезопасности, а также базовыми понятиями и правилами.