УТВЕРЖДЕНЫ
Решением Совета директоров
ДБ АО «Банк Хоум Кредит»
Протокол № 36/2020
от «26» октября 2020г.

Политика информационной безопасности Удостоверяющего центра ДБ АО «Банк Хоум Кредит»

Politics information security Certification Authority SB JSC "Bank Home Credit"

DIN PP00102

Алматы 2020 год

Справочная информация

Название:	**Политика информационной безопасности Удостоверяющего центра ДБ АО «Банк Хоум Кредит»**
Версия:	**2.00**
Подразделение – ответственный разработчик:	Департамент продаж
Уровень доступа:	**Общий**

Отв. разработчик:	**Должность**	**Ф.И.О.**	**Подпись**	**Дата**	**Конт. тел.**
	Менеджер по оптимизации процессов продаж	Реброва И.			2360

Хронология изменений и дополнений в документ

Ф.И.О. исполнителя	**Версия**	**Описание**	**Дата**
Реброва И.	1	Политика информационной безопасности Удостоверяющего центра ДБ АО «Банк Хоум Кредит»	17.04.2020г.

ОГЛАВЛЕНИЕ

1. Основные понятия 4
2. Общие положения..... 4
3. Описание информауионной безопасности.....5
3.1.Конфиденциальность.....5
3.1.1.Общие требования конфиденциальности.....5
3.1.2.Требования к обучению и осведомленности в вопросов информационной безопасности.....5
3.1.3.Требования по аутентификации пользователей.....5
3.1.4.Требования к серверным помещениям.....5
3.1.5.Контроль за обеспечением конфиденциальности.....6
3.1.6.Требования к используемой системы контроля и управления доступом.....6
3.2.Целостность.....6
3.2.1.Общие требования к целостности.....6
3.2.2.Требования к резервному копированию и восстановлению.....7
3.3.Доступность.....7
3.3.1.Общие требования.....7
3.3.2.Требования к отказоустойчивости.....7
3.3.3.Требования к бесперебойному питанию.....7
3.3.4.Требования по обеспечению резервирования и дублирования мощностей.....8
3.4.Требования к анализу и оценке рисков.....8
4.Ответсвенность.....8
5. Заключительные положения.....8

1. Основные понятия

1. В настоящей Политике информационной безопасности Удостоверяющего центра ДБ АО «Банк Хоум Кредит», используются следующие термины и сокращения:

1) **Авторизированные лица** - лица, имеющие право на работу с информационной системой в рамках своей компетенции (роли);

2) **Аутентификация** - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа реализованным в системе;

3) **Банк** - ДБ АО «Банк Хоум Кредит»;

4) **ВНД –** внутренний нормативный документ;

5) **Головной офис (ГО) Банка –** центральный, главный офис Банка в г. Алматы;

6) **Доступность информации** - состояние информации (ресурсов автоматизированной информационной системы), при которой субъекты, имеющие право доступа, могут реализовывать его беспрепятственно;

7) **Информационная безопасность (ИБ)** - состояние устойчивости (защищенности) Критичных Информационных активов Банка к случайным или преднамеренным воздействиям, исключающее недопустимые риски недоступности, уничтожения, искажения и раскрытия информации, которые приводят к материальному, репарационному или иному ущербу Банка, его акционеров, работников или клиентов;

8) **Инфраструктура Открытых Ключей (ИОК)** - комплекс информационных систем, организационных и технических мероприятий, направленный на управление регистрационными свидетельствами в соответствии с законодательством Республики Казахстан об электронном документе и электронной цифровой подписи;

9) **ИС** – информационная система;

10) **Конфиденциальность информации** - обеспечение предоставления информации только авторизированным лицам;

11) **ОС** – операционная система;

12) **ПО** –программное обеспечение;

13) **Пользователи ИОК** - лица, работающие с информацией в ИОК;

14) **Политика** - Политика информационной безопасности Удостоверяющего центра ДБ АО «Банк Хоум Кредит»;

15) **Работники Банка** - лица, работающие с информацией или другими объектами, относящимися к ИОК;

16) **Удостоверяющий центр (УЦ)** – Банка или иное юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

17) **УИБ** – Управление информационной безопасности Банка, отвечающее за обеспечение информационной безопасности ИОК;

18) **Целостность информации** - состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения

2. Нормативную правовую основу Политики составляют положения законодательства Республики Казахстан регулирующие вопросы по использованию информационных систем и информационной безопасности, требования международных стандартов управления информационной безопасностью, а также отношения в сфере информатизации и возникающих при создании и использовании электронных документов, удостоверенных посредством электронных цифровых подписей.

3. Настоящая Политика предназначена для определения целей, требований обеспечения ИБ ИОК.

4. Под обеспечением ИБ или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – обеспечение возможности получения доступа к данным авторизованным лицам в нужное для них время.

Целью обеспечения ИБ является минимизация ущерба от реализации угроз ИБ, а также повышение общего уровня конфиденциальности, целостности и доступности информации в ИОК.

5. Классификация информации в ИОК и уровень ее важности устанавливаются и регулируются в соответствии с законодательством Республики Казахстан.

3. Описание информационной безопасности

3.1. Конфиденциальность

3.1.1. Общие требования конфиденциальности

6. Главным требованием конфиденциальности является обеспечение предоставления информации УЦ только авторизированным лицам.

7. Защищаемая информация, обрабатываемая и хранящаяся в ИОК подлежит копированию и передаче третьему лицу только с официального разрешения руководства Банка.

8. Запись и копирование защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные носители информации.

9. При работе с ИОК должна исключаться возможность наблюдения за отображаемой информацией посторонними лицами.

10. При работе с ИОК должны использоваться специальные лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак, контроль за работой которых обеспечивается УИБ.

11. Явно не разрешенный доступ к информации ИОК является запрещенным.

12. Серверное оборудование УЦ должно находиться в выделенной подсети или виртуальной локальной сети.

13. При увольнении или переводе в другое структурное подразделение администратора УЦ, должны блокироваться или удаляться все учетные записи данного администратора для доступа к ИОК.

3.1.2. Требования к обучению и осведомленности в вопросах информационной безопасности

14. Работники, работающие с ИОК должны проходить регулярное обучение по вопросам ИБ.

3.1.3. Требования по аутентификации пользователей

15. Все пользователи, работающие в ИОК должны проходить безопасную аутентификацию, идентифицирующую их и исключающую возможность подбора пароля и перехвата авторизационных данных.

16. При работе с ИОК должно быть установлено ограниченное время соединения для пользователей (завершение работы при отсутствии активности пользователя).

3.1.4. Требования к серверным помещениям

17. Серверные помещения в которых размещаются сервера и активное сетевое оборудование, используемое для ИОК, должны иметь:

1) систему контроля и управления доступом (регистрация информации о работнике и времени посещения);
2) систему видеонаблюдения;
3) систему кондиционирования и вентиляции;
4) систему мониторинга микроклимата;
5) систему охранной сигнализации;
6) систему пожарной сигнализации;
7) систему газового пожаротушения;
8) систему газо- и дымоудаления.

3.1.5. Контроль за обеспечением конфиденциальности

18. С целью контроля за обеспечением конфиденциальности должны проводиться следующие мероприятия:
1) постоянный мониторинг инструментальными средствами ИБ серверов УЦ на попытки сетевых атак и вторжений;
2) ежегодная проверка наличия избыточных учетных записей в ИОК с их удалением в случае обнаружения.

3.1.6. Требования к используемой системы контроля и управления доступом

19. Система контроля и управления доступом (СКУД) — аппаратно-программный комплекс средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери подъезда, двери офисов и др.
Сервера и рабочие места работников УЦ оснащены аппаратно-программными комплексами защиты от несанкционированного доступа/съема информации ИОК.
20. СКУД должна обеспечивать управление доступом в помещения Банка:
1) ограничение доступа на заданное помещение;
2) идентификацию лица, имеющего доступ в заданное помещение.
21. СКУД может быть интегрирована с системой видеонаблюдения и пожарной сигнализацией Банка.
22. Уровень доступа работников в помещения Банка утверждается приказом директора Департамента безопасности Банка.

3.2. Целостность

3.2.1. Общие требования к целостности

23. Главным требованием целостности является обеспечение изменения информации ИОК только авторизированными лицами.
24. Действия и операции по изменению информации в ИОК должны фиксироваться с сохранением данной информации на срок не менее 5 лет.
25. Все новые версии программного обеспечения ИОК должны проходить тестирование в ДИТ и УИБ.
26. Установка новых версий программного обеспечения ИОК должна осуществляться администратором прикладного ПО и согласовываться с руководством Банка.
27. Закуп нового оборудования и ПО, для усовершенствования ИС ИОК производится по согласованию с руководством Банка.
28. При проведении проверок или аудитов ИОК должен предоставляться доступ только на чтение.

29. Силовые и телекоммуникационные линии, связывающие средства обработки информации, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой.

30. Сетевой кабель должен быть защищен от не авторизованных подключений или повреждения.

31. Силовые кабели должны быть отделены от коммуникационных, для предотвращения помех.

32. Необходимо применять легко распознаваемые маркировки на кабелях и оборудовании.

33. С целью указания достоверности времени ИОК должна использовать сетевой протокол для синхронизации часов.

3.2.2. Требования к резервному копированию и восстановлению

34. Резервному копированию подлежат файлы ОС и прикладное ПО ИОК.

35. Резервное копирование прикладного ПО должно производиться после каждого внесения изменения.

36. Носители с данными ПО должны храниться в запираемом металлическом шкафу.

37. При каждом изменении версии прикладного ПО (исправление ошибок, добавление функциональности), старая версия ПО должна сохраняться в течение 3 месяцев.

3.3. Доступность

3.3.1. Общие требования

38. Главным требованием доступности является обеспечение состояния информации ИОК (ресурсов автоматизированной информационной системы), при котором авторизированные лица могут работать с ней беспрепятственно.

39. На случай возникновения аварий, стихийных бедствий и иных внештатных ситуаций должны быть предусмотрены соответствующие меры защиты и обеспечения непрерывной работы и восстановления.

40. Аварии, стихийные бедствия и иные внештатные ситуации должны фиксироваться в журнале с сохранением данной информации на срок не менее 1 года.

3.3.2. Требования к отказоустойчивости

41. Аппаратно-программное обеспечение должно обеспечивать выполнение задач ИОК со временем однократного простоя не более 6 часов и суммарным временем простоя не более 48 часов в год.

42. В случае возникновения внештатной ситуации, произошедшей с производственным сервером УЦ, на восстановление системы должно быть затрачено не более 6-ти часов.

43. Резервное оборудование должно проходить тестирование не реже одного раза в год.

44. Резервные копии информации должны проходить тестирование не реже одного раза в месяц.

3.3.3. Требования по бесперебойному питанию

45. Бесперебойное электропитание обеспечивается источником бесперебойного питания необходимой мощности, который должен гарантировать, как минимум, корректное завершение работы приложений и операционной системы серверов при отключении внешнего электропитания.

3.3.4. Требования по обеспечению резервирования и дублирования мощностей

46. Система хранения данных должна предусматривать автоматический периодический контроль целостности дисков, анализ плохих секторов, без вмешательства администратора и без влияния на работу серверов УЦ.

47. Система хранения данных должна обеспечивать возможность «горячей» замены дисков.

3.3.5. Требования по обеспечению оперативного мониторинга состояния доступности

48. Должны быть предусмотрены средства оперативного мониторинга состояния доступности сервисов ИОК в режиме реального времени.

49. Должны быть установлены дополнительные программные модули, обеспечивающие составление отчетов в виде графиков на основе мониторинга загруженности серверов и их других основных параметров - свободное дисковое пространство, загрузки процессора, свободная оперативная память.

3.4. Требования к анализу и оценке рисков

50. Настоящая Политика ИБ ИОК должна основываться на данных, полученных в результате анализа и оценки рисков ИБ.

51. С целью совершенствования Политики ИБ, должен проводиться ежегодный анализ и оценка рисков ИБ для ИОК.

52. При оценке рисков должно учитываться влияние реализации угроз ИБ на финансовое состояние. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

4. Ответственность

53. Администраторы ИОК несут персональную ответственность за своевременное резервное копирование информации.

54. Администраторам ИОК запрещается разглашать любую конфиденциальную информацию, связанную с функционированием ИОК.

55. Все работники Банка должны следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации.

56. В случае нарушения требований данной Политики руководитель и работники Банка, работающие с ИОК привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

57. Руководитель ИОК несет ответственность за разработку и актуализацию настоящей Политики.

5. Заключительные положения

58. В целях реализации положений Политики Банком могут разрабатываться соответствующие ВНД.

59. Политика может быть пересмотрена в случае изменения структуры Банка, а также в иных случаях в соответствии с требованиями внутренних нормативных документов Банка, решениями уполномоченного органа Банка или требованиями законодательства Республики Казахстан.

60. Требования, изложенные в настоящем документе, обязательны для исполнения всеми работниками Банка, работающими с ИОК.

61. Контроль за исполнением требований настоящей Политики обеспечивают работники УИБ Банка.

62. Все лица причастные к функционированию ИОК, в случае имеющихся сведений о нарушениях требований данной Политики или других противоправных действий в отношении ИОК, должны поставить в известность руководителя УЦ и УИБ Банка.

63. Вопросы, не урегулированные Политикой, разрешаются в порядке, определенном законодательством Республики Казахстан и ВНД Банка.

64. С даты вступления в силу настоящей Политики, считать утратившим силу Политику информационной безопасности Удостоверяющего центра ДБ АО «Банк Хоум Кредит» (утвержденную решением Совета директоров ДБ АО «Банк Хоум Кредит», протокол № 13/2020 от 17.04.2020 г.