«Утверждено»
Решением Единственного участника
ТОО «Ломбард Верный»
Приказ № 01/02-1
от «22» апреля 2024 года

Политика информационной безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса и терминалов.

Алматинская область
2024 год

Предисловие

Введен: 22 апреля 2024 года.
Срок пересмотра: 2026 год или ранее в случае осуществляются в соответствии с изменениями в законодательстве Республики Казахстан и по мере необходимости.

Содержание

1. Общие положения

1. Настоящая Политика безопасности и защиты информации от несанкционированного доступа при предоставлении услуг через интернет-ресурсы (веб-сайт) и/или терминалов в ТОО "Ломбард Верный" (далее – Компания) разработана в соответствии с законодательством Республики Казахстан в области информационной безопасности, актами уполномоченного органа и внутренними документами организации.
2. Основная цель данной Политики заключается в минимизации ущерба от событий, которые могут угрожать безопасности информации, путем их предотвращения или сведения их последствий к минимуму. Обеспечение информационной безопасности не является целью само по себе; оно необходимо для снижения рисков и экономических потерь, связанных с различными угрозами, с которыми сталкиваются информационные ресурсы организации. Для этого важно поддерживать основные характеристики информации:

    - Доступность: обеспечение своевременного и беспрепятственного доступа к информации субъектам, обладающим соответствующими полномочиями.
    - Конфиденциальность: введение ограничений на круг лиц, имеющих доступ к информации, и обеспечение ее сохранности от доступа неуполномоченных лиц.
    - Целостность: сохранение информации в неизменном виде, не подвергая ее искажениям или изменениям относительно определенного состояния.

3. Данная Политика разработана на основании следующих документов:

– Постановление Правления Национального Банка Республики Казахстан от 28 ноября 2019 года № 217.

– ИСО/МЭК 27001:2022 Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования;

– ИСО/МЭК 27002:2022 Информационные технологии – Методы обеспечения безопасности – Правила и нормы управления информационной безопасностью.

4. Основными принципами Политики являются:
    - законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Компании;
    - ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности Компании;
    - непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Компании должны осуществляться без прерывания или остановки текущих бизнес-процессов Компании;
    - комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
    - обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны

соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;

- приоритетность – категорирование (ранжирование) всех информационных ресурсов Компании по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности.

5. Настоящая Политика определяет:
   - Основные меры по обеспечению информационной безопасности Компании, в том числе минимизация угроз информационной безопасности, т. е. совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;
   - способы двухфакторной аутентификации и верификации потенциальных заемщиков посредством интернет-ресурса, терминалов и (или) сайта;
   - обеспечение безопасного хранения электронных сообщений и иных документов, предоставленных заемщику и полученных от него, с соблюдением их целостности и конфиденциальности в течение не менее 5 (пяти) лет после прекращения обязательств сторон по договору о предоставлении микрокредита;
   - меры для профилактики замышляемых правонарушений со стороны третьих лиц.
6. Положения настоящей Политики распространяются на следующий перечень объектов:
   - работники структурных подразделений Компании (в том числе стажеры, практиканты);
   - заемщики Компании и иные третьи лица, имеющие доступ к информационным системам и документам Компании, в той их части, которая непосредственно взаимосвязана с Компании и их деятельностью;
   - поставщики, третьи лица и стороны, имеющие договорные отношения с Компании;
   - информационные ресурсы Компании, составляющие конфиденциальную информацию, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности, информационные ресурсы (базы данных, файлы, системная документация, руководства пользователя, учебные материалы, политики и процедуры и т. п.), в том числе общедоступная информация, представленная в электронном виде;
7. информационная инфраструктура Компании, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, носители информации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы IT ресурсов.
8. **Настоящая Политика является общедоступным документом и размещается на официальном Интернет-ресурсе Компании** https://tezbai.kz/
9. Процесс создания надежной информационной защиты никогда не бывает законченным. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды.

2. Меры обеспечения информационной безопасности

10. Основными мерами по обеспечению информационной безопасности Компании являются:
    - административно-правовые и организационные меры;
    - меры физической безопасности;
    - программно-технические меры.

10.1. Административно-правовые и организационные меры включают (но не ограничены ими):
- контроль исполнения требований законодательства РК и внутренних документов;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
- контроль соответствия бизнес-процессов требованиям Политики;
- информирование и обучение работников Компании работе с информационными системами и требованиям информационной безопасности;
- реагирование на инциденты, локализацию и минимизацию последствий;
- анализ новых рисков информационной безопасности;
- отслеживание и улучшение морально-делового климата в коллективе;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников Компании.

10.2. Меры физической безопасности включают (но не ограничены ими):
- организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
- организацию противопожарной безопасности охраняемых объектов;
- контроль доступа работников Компании и третьих лиц в помещения ограниченного доступа (сервер).

10.3. Программно-технические меры включают (но не ограничены ими):
- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- применение комплексной антивирусной защиты;
- использование средств защиты периметра (фаерволл, антивирус и т. п.);
- использование средств информационной безопасности, встроенных в информационные системы;
- обеспечение регулярного резервного копирования информации;
- контроль за правами и действиями пользователей, в первую очередь, привилегированных;
- применение систем криптографической защиты информации;
- обеспечение безотказной работы аппаратных средств.
- анализ исходного кода, компонентов и библиотек с использованием сканера статического анализа исходных кодов, поддерживающего анализ всех используемых языков программирования в проверяемом программном обеспечении.

3. Оценка рисков информационной безопасности

11. Для оценки рисков информационной безопасности Компании проводятся следующие мероприятия:
    - формирование перечня критичных информационных активов;
    - оценка рисков информационной безопасности для критичных информационных активов.
12. В перечень критичных информационных активов включаются информационные активы, убытки от нарушения свойств которых превышают установленный уровень существенности убытков от нарушения информационной безопасности.
13. В целях осуществления оценки рисков информационной безопасности для критичных информационных активов Компании обеспечивает реализацию следующих процессов:
    - идентификация угроз информационной безопасности критичным информационным активам;
    - идентификация источников угроз информационной безопасности, релевантных для критичных информационных активов;
    - идентификация уязвимостей критичных информационных активов;
    - идентификация существующих мер управления рисками информационной безопасности;
    - оценка вероятности реализации угроз информационной безопасности критичным информационным активам источниками угроз информационной безопасности;
    - оценка уровня рисков информационной безопасности.
14. Идентификация угроз информационной безопасности критичным информационным активам осуществляется подразделением по информационной безопасности. Для каждого критичного информационного актива анализируются угрозы информационной безопасности.
15. Идентификация источников угроз информационной безопасности, релевантных для критичных информационных активов, осуществляется подразделением по информационной безопасности Компании с учетом источников угроз информационной безопасности.
16. Идентификация уязвимостей критичных информационных активов осуществляется подразделением по информационной безопасности Компании, с учетом следующей информации о (об):
    - конструкции информационного актива;
    - физическом расположении информационного актива;
    - известных ошибках в программном коде;
    - ошибках в конфигурации;
    - недостатках процесса эксплуатации информационного актива.
17. Идентификация существующих мер управления рисками информационной безопасности для критичных информационных активов осуществляется подразделением по информационной безопасности, с учетом информации об организационных и технических мероприятиях, направленных на исправление существующих недостатков в процессе обеспечения информационной безопасности критичных информационных активов либо последствий ее нарушения.
18. Оценка вероятности реализации угроз информационной безопасности критичным информационным активам источниками угроз информационной безопасности осуществляется подразделением по информационной безопасности для всех релевантных для критичного информационного актива комбинаций источника угрозы информационной безопасности, угрозы информационной безопасности и уязвимости, с учетом следующей информации:

- данные о расположении источника угрозы информационной безопасности относительно соответствующих критичных информационных активов (внутренний или внешний). Для внутренних источников угроз информационной безопасности учитывается количество пользователей актива, для внешних источников угроз информационной безопасности - наличие возможного доступа извне периметра защиты;
- данные об уровне доступа источника угрозы информационной безопасности;
- статистические данные о частоте реализации угрозы информационной безопасности критичному информационному активу в прошлом;
- информация о сложности реализации угрозы информационной безопасности критичному информационному активу;
- данные о наличии у рассматриваемых критичных информационных активов защитных мер.

19. При привлечении к оценке вероятности реализации угрозы информационной безопасности критичным информационным активам источниками угроз информационной безопасности нескольких экспертов и получении разных оценок итоговая, обобщенная оценка принимается равной оценке, определяющей наибольшую вероятность.
20. Оценка уровня рисков информационной безопасности проводится на основании сопоставления оценок вероятности реализации угрозы информационной безопасности критичным информационным активам источниками угроз информационной безопасности и оценок соответствующих потенциальных убытков от нарушения конфиденциальности, целостности или доступности критичного информационного актива.

4. Требования к автоматизированной информационной системе

21. Автоматизированная информационная система включает:

1) программное обеспечение серверов веб-приложений (далее – веб-приложение);

2) программное обеспечение серверов программных интерфейсов (далее – серверное ППО).

22. Разработка и (или) доработка автоматизированной информационной системы осуществляется Компанией, в соответствии с внутренним документом, регламентирующим порядок разработки и (или) доработки, этапы разработки и их участников.

23. Хранение исходных кодов автоматизированной информационной системы, разрабатываемых в Компании, осуществляется в специализированных системах управления репозиториями кода, размещаемых в периметре защиты Компании, с обеспечением резервного копирования.

24. Обязательным этапом является тестирование безопасности, в ходе которого осуществляются, как минимум, следующие мероприятия:

1) статический анализ исходного кода;

2) анализ компонентов и сторонних библиотек.

25. Статический анализ исходного кода автоматизированной информационной системы, проводится с использованием сканера статического анализа исходных кодов, поддерживающего анализ всех используемых языков программирования в проверяемом программном обеспечении, в функции которого входит выявление следующих уязвимостей, но не ограничиваясь:

1) наличие механизмов, допускающих инъекции вредоносного кода;

2) использование уязвимых операторов и функций языков программирования;

3) использование слабых и уязвимых криптографических алгоритмов;

4) использование кода, вызывающего при определенных условиях отказ в обслуживании или существенное замедление работы приложения;

5) наличие механизмов обхода систем защиты приложения;

6) использование в коде секретов в открытом виде;

7) нарушение шаблонов и практик обеспечения безопасности приложения.

26. Анализ компонентов и (или) сторонних библиотек автоматизированной информационной системы, проводится с целью выявления известных уязвимостей, присущих используемой версии компонента и(или) сторонней библиотеки, а также отслеживания зависимостей между компонентами и (или) сторонними библиотеками и их версиями.

27. Компания обеспечивает реализацию корректирующих мер по устранению выявленных уязвимостей в порядке, определенном внутренним документом, при этом критичные уязвимости устраняются до ввода в эксплуатацию автоматизированной информационной системы и (или) ее новых версий.

28. Компания обеспечивает хранение и доступ в оперативном режиме ко всем версиям исходных кодов автоматизированной информационной системы и результатов тестирования безопасности, которые были введены в эксплуатацию в течение последних 3 (трёх) лет.

29. Обмен данными между клиентской и серверной сторонами автоматизированной информационной системы шифруется с использованием версии протокола шифрования Transport Layer Security (Транспорт Лэйер Секьюрити) не ниже 1.2.

30. Веб-приложение обеспечивает:

1) однозначность идентификации принадлежности веб-приложения Компании (доменное имя, логотипы, корпоративные цвета);

2) запрет на сохранение в памяти браузера авторизационных данных;

3) маскирование вводимых секретов;

4) информирование на странице авторизации клиента о мерах обеспечения кибергигиены, которым рекомендуется следовать при использовании веб-приложения;

5) обработку ошибок и исключений безопасным способом, не допуская отображение в интерфейсе клиента конфиденциальных данных, предоставляя минимально достаточную информацию об ошибке.

31. Доступ к информации в автоматизированной информационной системе предоставляется работникам Компании, в объеме, необходимом для исполнения их функциональных обязанностей.

32. Доступ к автоматизированной информационной системе осуществляется путем идентификации и аутентификации работников Компании.

33. В автоматизированной информационной системе применяются функции по управлению учетными записями и паролями, а также блокировке учетных записей пользователей, определяемые внутренним документом Компании.

34. Автоматизированная информационная система обеспечивается технической поддержкой, в состав которой входят услуги по предоставлению обновлений автоматизированной информационной системы, в том числе обновлений безопасности.

35. Автоматизированная информационная система обеспечивает резервное хранение данных, файлов и настроек, которое обеспечивает восстановление ее работоспособной копии.

36. В Компании обеспечивается ведение и неизменность аудиторского следа автоматизированной информационной системы, как на организационном, так и на техническом уровне.

37. Для защиты автоматизированной информационной системы используется лицензионное антивирусное программное обеспечение или системы, обеспечивающие целостность или контроль неизменности программной среды на рабочих станциях, ноутбуках и мобильных устройствах.

38. Компания обеспечивает безопасное хранение электронных сообщений и иных документов, предоставленных клиенту и полученных от него, с соблюдением их целостности и конфиденциальности в течение не менее 5 (пяти) лет после прекращения обязательств сторон по договору о предоставлении микрокредита.

Хранение электронных сообщений и иных документов осуществляется в том формате, в котором они были сформированы, отправлены клиенту или получены от него.

5. Безопасное хранение электронных сообщений и иных документов

39. В целях обеспечения информационной безопасности в Компании выполняются следующие условия:

- по организации системы управления информационной безопасностью;
- по организации доступа к информационным активам;
- по обеспечению безопасности информационной инфраструктуры;
- по осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;
- по проведению анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;
- по средствам криптографической защиты информации;
- по обеспечению информационной безопасности при доступе третьих лиц к информационным активам;
- по проведению внутренних проверок состояния информационной безопасности;
- по процессам системы управления информационной безопасностью.

40. Подлежащая защите информация может:

- размещаться на бумажных носителях;
- существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);
- передаваться по телефону, телефаксу, телексу и т. п. в виде электрических сигналов;
- присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

41. Требования к обеспечению информационной безопасности при организации деятельности Компании в части договоров на предоставление сведений о потенциальных заемщиках (данные об официальных доходах, перечислениях из ГФСС, о количестве и средней сумме пенсионных выплат из республиканского бюджета, данных кредитного отчета и другие отчеты) от кредитного бюро (далее по тексту - КБ) в рамках заключенных договоров:

a. Компания обеспечивает конфиденциальность и целостность информации, получаемой из информационной системы КБ.

b. Компания обеспечивает надлежащий уровень информационной безопасности в соответствии с условиями Договоров, заключенных с КБ.

c. Компания обеспечивает исполнение организационно-технических, технологических требований и мер, необходимых для функционирования и защиты системного и прикладного программного обеспечения, используемого для взаимодействия с информационной системой КБ и обработки, получаемой из нее информации.

d. При использовании оборудования для работы с информационной системой КБ учитывается необходимость его защиты от несанкционированного доступа, а также защиты носителей информации и сетевых ресурсов, используемых для работы с информационной системой КБ.

e. Компания определяет и утверждает перечень ответственных лиц.

f. Компания обеспечивает наличие подписанных ответственными (ответственным) лицами (лицом) организации обязательств о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими функциональных обязанностей.

g. Компания обеспечивает наличие внутренних документов, определяющих порядок определения и утверждения перечня ответственных лиц, их права и ответственность (включая должностные инструкции).

h. Доступ к информации предоставляется работникам Компании в объеме, необходимом для исполнения их функциональных обязанностей.

i. Учетная запись ответственного лица, по которой он идентифицируется в информационной системе КБ, соответствует конкретному физическому лицу (оператор).

j. Компания проводит плановые и внеплановые проверки соответствия рабочих станций (сайтов, мобильных приложений, сайта) Политике информационной безопасности.

k. Компания по запросу уполномоченного органа представляет сведения, подтверждающие его соответствие требованиям, предусмотренным в договорах с КБ.

l. Операционная система рабочей станции обеспечивает функции идентификации и аутентификации пользователя, а также разграничения прав доступа пользователей и авторизации в соответствии с назначенными правами.

m. Компания использует собственную рабочую станцию.

n. При использовании рабочей станции для подключения к информационной системе Кредитного бюро одновременное подключение к другим ресурсам сети интернет не производится.

o. Работники Компании обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к информационным системам.

p. Работники Компании обеспечивают конфиденциальность информации, ставшей им известной в процессе использования информационной системы Кредитного бюро.

42. Ответственность за обеспечение информационной безопасности Компании возлагается на все структурные подразделения Компании в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами.

43. За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами Компании и законодательством РК.

6. Меры профилактики нарушений информационной безопасности

44. В профилактике инцидентов кибербезопасности важную роль играет соблюдение соответствующих национальных и международных требований при разработке программного обеспечения, проектировании компонентов информационных систем и инфраструктуры финансового сектора. Компания выполняет регулярную оценку рисков кибербезопасности, которая служит основой для выработки и применения мер по минимизации данных рисков, а также оценки эффективности реализованных мер.

45. Учитываются результаты, полученные на этапе профилактики (предотвращения), а также опыт уже обработанных инцидентов. Своевременно оценивается характер, масштабы и последствия инцидентов кибербезопасности, в целях снижения результатов их воздействия, своевременно уведомляются внутренние и внешние заинтересованные стороны и координируются совместные действия по реагированию. К заинтересованным сторонам относятся:

- Национальный Банк Республики Казахстан;
- иные уполномоченные государственные и законодательные органы, осуществляющие регулирование деятельности Компании;
- заемщики;
- кредиторы и инвесторы;
- работники структурных подразделений, осуществляющие взаимодействие в процессе осуществления деятельности Компании;
- поставщики услуг.

46. Обеспечивается продолжение операционной деятельности после инцидента при одновременном выполнении процедур восстановления, в том числе:

- устранения последствий инцидента;
- восстановления нормального состояния информационных систем и данных с подтверждением их нормального состояния;
- выявления и устранения уязвимостей, которые были использованы в рамках инцидента, в целях недопущения подобных инцидентов в будущем;
- обеспечения надлежащего информационного обмена внутри страны и за ее пределами.

47. Повышение информированности и компетенции, как пользователей, так и работников (повышение квалификации, обучение) помогут устранить риски и создать культуру безопасного создания и использования информации в Компании. На этапе повышения осведомленности следует использовать опыт, полученный в ходе профилактики и реагирования, чтобы пользователи были ознакомлены с реальными рисками и эффективными методами их минимизации.

48. Классическая модель информационной безопасности базируется на обеспечении трех значимых для безопасности информации атрибутов: конфиденциальность, целостность и доступность.

49. Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.

50. Если доступ к информации получает неуполномоченное лицо, происходят несанкционированный доступ или нарушение конфиденциальности.

51. Доступность (возможность за разумное время получить требуемую информационную услугу)

52. Целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

53. В случае обнаружения несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, ее несанкционированного изменения, осуществления несанкционированных действий со стороны третьих лиц, Компания незамедлительно принимает меры для устранения причин и последствий таких действий, а также в течение одного рабочего дня информирует об этом уполномоченный орган.

54. Компания принимает меры по предотвращению использования действующих или внедряемых способов и технологий предоставления микрокредитов электронным способом в

схемах легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма. При предоставлении микрокредитов и проведении кредитного скоринга потенциального заемщика Компания применяет необходимые меры, предусмотренные Законом Республики Казахстан от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон о ПОДФТ), а также в соответствии с Постановлением Правления Национального Банка Республики Казахстан О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 25 декабря 2013 года № 292 "О введении ограничений на проведение отдельных видов банковских и других операций финансовыми организациями".