ТУРБОЗАЙМ

УТВЕРЖДЕНО
Приказом Генерального директора
от 09.06.2025 № ТЗ-1551

СТАНДАРТ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ С КОНТРАГЕНТАМИ ООО МКК ТУРБОЗАЙМ

Москва, 2025

1. Термины и определения

Наименование термина	Определение термина
Конфиденциальная информация	Вся письменная или устная информация, а также информация, переданная в электронной форме, в отношении которой законами предусмотрен режим ограниченного доступа, либо информация, о которой раскрывающая ее сторона уведомила получающую сторону явным образом, что такая информация является конфиденциальной и требует защиты. К конфиденциальной информации относятся, в том числе, персональные данные и сведения, составляющие коммерческую, профессиональную, служебную, а также иные виды тайн, определенные действующим законодательством Российской Федерации, бухгалтерские и финансовые данные, информация о проведении платежных операций, информация о настройках информационных, телекоммуникационных и платежных систем, а также реквизиты доступа к ним.
Информационная система	Совокупность взаимосвязанных компонентов, которые используются для сбора, обработки, хранения и передачи информации. К компонентам информационной системы, например, относятся: – компьютеры, серверы (в том числе виртуальные) и системы хранения данных; – сетевое и телекоммуникационное оборудование; – программное обеспечение, обеспечивающее функционирование компонентов информационной системы; – обрабатываемая информация и данные, в том числе технического характера (конфигурации, описания процессов и сценарии использования компонент и проч.).
Информационное взаимодействие	Обмен и совместная обработка конфиденциальной информации, а также совместное использование (разработка, обслуживание, администрирование и проч.) информационных систем, в которых обрабатывается конфиденциальная информация.
Аутентификационные данные	Информация, используемая для проверки подлинности пользователя, службы или сервиса, например: – логин и пароль учетной записи; – ключи доступа к API (API-key); – криптографические ключи, применяющиеся для аутентификации пользователей, сетевых запросов и защиты информации при ее передаче по телекоммуникационным сетям.
Реквизиты доступа	Информация, используемая для установления соединения с информационной системой, службой или сервисом. К ней относятся аутентификационные данные, а также данные, идентифицирующие конкретные информационную систему, службу или сервис среди других и с использованием которых устанавливается сетевое соединение, например: - IP-адрес; - порт; - имя хоста.
Информационная безопасность	Состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, целостность и доступность, а также такие свойства, как подлинность, неотказуемость, достоверность.

2. Общие положения

2.1. Настоящий Стандарт по обеспечению информационной безопасности при взаимодействии с контрагентами ООО МКК Турбозайм (далее – «Стандарт») регулирует правила обеспечения информационной безопасности и защиты интересов общества с ограниченной ответственностью микрокредитная компания «Турбозайм» (далее по тексту – «Компания») и третьих лиц (поставщики, продавцы, исполнители, подрядчики, арендодатели и др.) (далее совместно именуемых «Контрагенты», а по отдельности – «Контрагент»), участвующих в информационном взаимодействии с Компанией при заключении и исполнении обязательств и сделок, в том числе, включая, но, не ограничиваясь поставку, аренду, оказание услуг, подряд и прочее, (далее совместно именуемые «Сделки», а по отдельности – «Сделка»).

2.2. Для целей настоящего Стандарта Компания и Контрагент совместно именуются «Стороны», а по отдельности – «Сторона». В зависимости от контекста, словосочетания «Раскрывающая Сторона», либо «Получающая Сторона» могут обозначать как Компанию, так и Контрагента.

2.3. Целью настоящего Стандарта является обеспечение безопасности конфиденциальной информации Сторон, в том числе информационных систем, с использованием которых обрабатывается конфиденциальная информация Сторон.

2.4. Стороны гарантируют и подтверждают, что обязуются соблюдать указанные в настоящем Стандарте технические и организационные меры обеспечения информационной безопасности (далее совместно именуемые «Меры защиты информации», а по отдельности – «Мера защиты информации») в той степени, в какой они применимы к процессам исполнения Сделки, а также при экономической целесообразности их исполнения. При этом Стороны признают, что отказ от соблюдения той или иной Меры защиты информации не должен противоречить требованиям законодательства Российской Федерации.

2.5. Контрагенты обязуются применять настоящий Стандарт, в том числе при взаимодействии с третьими лицами (субподрядчиками), которые привлекаются Контрагентами для исполнения условий Сделки с Компанией и хранят, обрабатывают или получают доступ к информационным системам и конфиденциальной информации Компании (далее – Субподрядчики).

2.6. Стороны соглашаются с тем, что Субподрядчики обязаны соблюдать Меры защиты информации на условиях настоящего Стандарта.

2.7. Стороны имеют право запрашивать друг у друга подтверждение реализации Мер защиты информации. Для этого запрашивающая подтверждение Сторона должна предоставить второй Стороне соответствующий письменный запрос, а вторая Сторона должна предоставить в течение 5 (пяти) рабочих дней подтверждение реализации Мер защиты информации. Подтверждением реализации указанных в Стандарте Мер защиты информации является заполненный Контрольный лист соответствия требованиям информационной безопасности, форма которого приведена в Приложении к настоящему Стандарту.

3. Меры обеспечения информационной безопасности

3.1. Для достижения целей настоящего Стандарта Сторонам необходимо реализовать следующие технические Меры защиты информации:

3.1.1. Меры по защите конфиденциальной информации от несанкционированного доступа (НСД):

– осуществлять регулярное обновление системного и прикладного программного обеспечения, а также средств защиты информации, использующихся на автоматизированных рабочих местах и серверах (далее – Средства обработки информации);

– организовать раздельное хранение конфиденциальной информации, полученной и/или обрабатываемой в рамках взаимодействия с разными контрагентами;

– осуществлять блокирование Средств обработки информации в случае необходимости оставления их без контроля пользователя;

– осуществлять такое расположение экрана/монитора Средств обработки информации, которое будет исключать возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;

– при настройке прав доступа к Средствам обработки информации обеспечивать соблюдение принципа наименьших привилегий, согласно которому доступ пользователей ограничивается только информацией, системами и другими ресурсами, необходимыми пользователям для выполнения своих задач.

3.1.2. Меры по парольной защите конфиденциальной информации:

– доступ ко всем Средствам обработки информации, на которых обрабатывается конфиденциальная информация, должен быть защищен паролем. Беспарольный вход в операционную систему на таких устройствах должен быть запрещен настройками операционной системы или средств защиты информации;

– использовать стойкие к перебору пароли или многофакторную аутентификацию;

– запретить использование одного и того же пароля для доступа к нескольким информационным системам или Средствам обработки информации, за исключением случаев, когда применяются технологии единого входа (Active Directory, Lightweight Directory Service и прочие);

– при эксплуатации информационных систем не использовать пароли по умолчанию, установленные разработчиками программного и аппаратного обеспечения, использующегося в информационной системе. При наличии технической возможности, производить удаление или блокирование встроенных по умолчанию учетных записей и заменять их новыми учетными записями, с аналогичными правами;

– осуществлять периодическую смену паролей доступа к Средствам обработки информации и в информационные системы;

– внедрить процедуру внеплановой смены паролей в случае их компрометации, подозрении в компрометации или увольнения сотрудника, использовавшего пароли. Пароли доступа к общим, не персонифицированным, учетным записям, известные уволенным сотрудникам, должны изменяться после увольнения;

– обеспечивать защиту паролей при их передаче, хранении и использовании (вводе), исключать их подсматривание и перехват;

– осуществлять контроль жизненного цикла учетных записей работников в информационных системах и Средствах обработки информации. В рамках данного мероприятия должны блокироваться или удаляться учетные записи уволенных сотрудников и сотрудников, находящихся в длительных отпусках/больничных, а также осуществляться проверка учетных записей, не используемых продолжительное время;

– вести строгий учет учетных записей тестовых пользователей, а также не персонифицированных учетных записей приложений и служб.

3.1.3. Меры по антивирусной защите информации:

– использовать антивирусную защиту Средств обработки информации и следить за актуальностью антивирусных баз;

– контролировать работоспособность антивирусного программного обеспечения, проводить его периодическое тестирование;

– проводить антивирусную проверку всех файлов, полученных из внешних источников, и любых дистрибутивов программ, устанавливаемых на устройства, обрабатывающие конфиденциальную информацию.

3.1.4. Меры по защите информации при работе в сетях общего пользования (Интернет):

– использовать средства межсетевого экранирования. К таким средствам относятся специализированные устройства или программное обеспечение (устанавливаемое

дополнительно или встроенное в операционную систему), предназначенные для контроля и фильтрации проходящего через них сетевого трафика;

– не осуществлять работу в сетях общего пользования при отключенных средствах защиты информации (межсетевой экран, антивирус и проч.);

– при передаче конфиденциальной информации через сети общего пользования использовать методы и средства ее криптографической защиты и следить за актуальностью и безопасностью используемых для этого криптографических ключей;

– не хранить конфиденциальную информацию на некорпоративных облачных хранилищах, за исключением случаев аренды серверных мощностей и ресурсов в центрах обработки данных для корпоративного использования;

– при удаленной работе с конфиденциальной информацией обеспечивать безопасность сетевых соединений к Средствам обработки информации с использованием криптографических методов и технологии VPN.

3.1.5. Меры по обеспечению физической безопасности:

– минимизировать случаи переноса информации на материальные носители (флеш-накопители, карты памяти, оптические диски, бумага и проч.). Данная процедура должна быть разрешена для выполнения только в исключительных случаях;

– помещения, в которых располагаются Средства обработки информации и материальные носители конфиденциальной информации, должны обеспечивать контроль физического доступа в них;

– в целях предупреждения перебоев в обработке информации или физической утраты данных, должны применяться меры противопожарной безопасности, резервного копирования данных, резервирования источников питания Средств обработки информации;

– должно осуществляться гарантированное уничтожение информации на материальных носителях информации после окончания ее обработки или в случаях выхода из строя компонентов Средств обработки информации (жесткие диски, SSD и проч.).

3.1.6. Меры по реагированию на инциденты информационной безопасности:

– должны быть внедрены механизмы регистрации событий информационной безопасности и их анализа;

– должны быть внедрены процедуры обнаружения и регистрации инцидентов информационной безопасности, а также реагирования на них;

– должно осуществляться незамедлительное уведомление Сторон об инцидентах информационной безопасности, касающихся конфиденциальной информации Сторон, и предоставление информации о результатах расследования причин и условий возникновения таких инцидентов;

– информация об инцидентах информационной безопасности должна быть отнесена к конфиденциальной информации и не должна разглашаться без предварительного согласования Сторонами, кроме случаев, предусмотренных законодательством.

3.2. Для достижения целей настоящего Стандарта Сторонам необходимо реализовать следующие организационные Меры защиты:

3.2.1. Определить лицо, отвечающее за информационную безопасность, в чьи полномочия входит определение/согласование способов и методов защиты информации, а также взаимодействие с внешними контрагентами и государственными органами по вопросам информационной безопасности.

3.2.2. Утвердить и соблюдать задокументированные политики, стандарты и регламенты, касающиеся:

– определения способов и периодичности повышения осведомленности работников в вопросах обеспечения информационной безопасности;

– регламентации процессов антивирусного контроля информационных систем;

– обращения с паролями и аутентифицирующей информации;

– разграничения доступа к информационным системам;

– контроля защищенности и устранения уязвимостей информационных систем;

– регистрации событий информационной безопасности и реагирования на инциденты информационной безопасности;

– криптографической защиты информации при ее передаче по не доверенным каналам связи;

– обеспечения сетевой безопасности, в том числе вопросов безопасной работы в сети Интернет и с электронной почтой;

– использования работниками личных устройств для работы со служебной информацией;

– обеспечения физической безопасности помещений, средств обработки и материальных носителей информации.

3.2.3. Проводить мероприятия по повышению осведомленности своих работников в области информационной безопасности, в том числе по вопросам противодействия фишингу и социальной инженерии.

3.2.4. Вести учет и контроль процедур обработки конфиденциальной информации, по возможности сводить их к минимуму.

3.3. Стороны должны обеспечить подписание своими работниками обязательств о неразглашении конфиденциальной информации, к которой работники получают доступ в процессе исполнения своих должностных обязанностей. Работники Сторон, не подписавшие такие обязательства, не должны допускаться к работе с конфиденциальной информацией.

3.4. Стороны должны следить за актуальностью и периодически обновлять перечисленные в п. 3.2.2 настоящего Стандарта политики, процедуры и регламенты, в случае изменения законодательства и/или процессов обработки информации.

3.5. Контрагенты, предоставляющие услуги, связанные с программными продуктами собственной разработки, такие как поставка программных продуктов, предоставление услуг и сервисов с применением программных продуктов собственной разработки и прочие, обязаны:

3.5.1. Обеспечивать безопасное проектирование, разработку, тестирование, поставку и сопровождение таких программных продуктов;

3.5.2. Обеспечивать наличие и функционирование процессов безопасной разработки; при этом желательно наличие формализованной политики, регламентирующей безопасную разработку;

3.5.3. Проводить обязательный анализ безопасности программного обеспечения, включающий статический анализ исходного кода, проверку на наличие жёстко заданных конфиденциальных, идентификационных данных и анализ сторонних компонентов;

3.5.4. Обеспечивать не только использование средств анализа безопасности, но и наличие налаженного процесса своевременного устранения выявленных уязвимостей;

3.5.5. Вести статистику по выявленным уязвимостям на каждом этапе анализа безопасности программного обеспечения (отдельно по результатам статического анализа, анализа сторонних компонентов и проверки на наличие конфиденциальных данных), включающую как минимум сведения о количестве выявленных уязвимостей критического и высокого уровней значимости; при этом конкретные уязвимости не раскрываются.

3.5.6. Предоставлять пользователям программных продуктов собственной разработки перечень зависимостей, необходимых для функционирования программных продуктов, и рекомендации по безопасной настройке и использованию программных продуктов.

4. Ответственность

4.1. Стороны несут ответственность за соблюдение требований настоящего Стандарта.

4.2. В случае нарушения либо подозрения на нарушение одной из Сторон требований настоящего Стандарта вторая Сторона вправе приостановить информационное взаимодействие с другой Стороной, а также прекратить ее доступы к своим информационным системам, до момента устранения нарушений.

4.3. В случае повторного нарушения одной из Сторон требований настоящего Стандарта вторая Сторона вправе расторгнуть Сделку.

4.4. В случае нарушения требований Стандарта Компания имеет право потребовать от Контрагента компенсации ущерба, причиненного последним вследствие нарушения или неисполнения требований Стандарта.

4.5. Контрагенты несут ответственность за применение положений настоящего Стандарта при взаимодействии с Субподрядчиками.

5. Иные условия

5.1. Настоящий Стандарт подлежит публикации на сайте Компании в сети Интернет по адресу https://turbozaim.ru.

5.2. Положения настоящего Стандарта доводятся до Контрагентов, участвующих в информационном взаимодействии с Компанией, путем включения ссылки на него и обязательств по его исполнению в договоры, соглашения, контракты или другие документы, составляемые при оформлении Сделок и содержащие их условия.

5.3. При необходимости, настоящий Стандарт может быть включен в виде приложения в договоры, соглашения, контракты или другие документы, составляемые при оформлении Сделок и содержащие их условия.

5.4. Положения настоящего Стандарта обновляются и пересматриваются по мере необходимости.

5.5. Изменения в настоящий Стандарт вносятся и публикуются следующим образом:

5.5.1. Компания вправе в одностороннем порядке вносить изменения в настоящий Стандарт. При внесении изменений в актуальной редакции указывается дата последнего обновления и номер редакции.

5.5.2. Новая редакция Стандарта вступает в силу с момента её размещения на сайте Компании, если иное не предусмотрено новой редакцией Стандарта.

5.5.3. Контрагенты, в условиях Сделок с которыми внесены обязательства по соблюдению положений настоящего Стандарта, уведомляются об изменении текста Стандарта путём размещения новой редакции Стандарта на сайте Компании. Предыдущие редакции Стандарта хранятся в архиве Компании.

Приложение
к Стандарту по обеспечению информационной безопасности при взаимодействии с контрагентами ООО МКК Турбозайм

Форма Контрольного листа соответствия требованиям информационной безопасности

----------*(начало формы)*----------

Утверждаю
Генеральный директор
(подпись) *ФИО*
М.П.

КОНТРОЛЬНЫЙ ЛИСТ
соответствия требованиям информационной безопасности

Компания:	*<Указывается наименование компании, в которой проводится контроль>*
Цель контрольных мероприятий:	Подтверждение соответствия технических и организационных мер обеспечения информационной безопасности Компании требованиям Стандарта по обеспечению информационной безопасности при взаимодействии с контрагентами ООО МКК Турбозайм.
Основание проведения контроля	Договор от *<указывается дата договора>* № *<указывается номер договора>* между Компанией и ООО МКК Турбозайм на выполнение работ/услуг по *<указывается предмет договора>.*
Дата проведения контроля:	__.__.20__ г.

Мера защиты информации	Описание меры	Выполняется (да/нет)	Комментарий[1]
Защита конфиденциальной информации от НСД	Регулярное обновление системного и прикладного программного обеспечения, а также средств защиты информации		
	Раздельное хранение конфиденциальной информации, полученной и/или обрабатываемой в рамках взаимодействия с разными контрагентами		
	Блокирование средств обработки информации в случае необходимости оставления их без контроля пользователя		
	Экраны/мониторы средств обработки информации расположены так, что исключается возможность несанкционированного ознакомления с отображаемой на них информацией		

[1] В случае если мера не выполняется, в поле «Комментарий» обязательно необходимо указать обоснование отказа от реализации меры. Комментарий также необходимо оставлять в случае частичного исполнения меры.

	посторонними лицами		
	Настройка прав доступа к средствам обработки информации осуществляется соблюдением принципа наименьших привилегий		
Парольная защита конфиденциальной информации	Доступ ко всем автоматизированным рабочим местам и серверам, на которых обрабатывается конфиденциальная информация, защищен паролем, а беспарольный вход в операционную система таких устройств запрещен		
	Используются стойкие к перебору пароли или многофакторная аутентификация		
	Запрещено использование одного и того же пароля для доступа к нескольким информационным системам или средствам обработки информации		
	Не используются пароли по умолчанию, установленные разработчиками программного и аппаратного обеспечения, производится удаление/блокирование встроенных по умолчанию учетных записей		
	Осуществляется периодическая смена паролей		
	Производится внеплановая смена паролей в случае их компрометации, подозрении в компрометации или увольнения сотрудника, использовавшего пароли		
	Обеспечивается защита паролей при их передаче, хранении и использовании (вводе), исключены их подсматривание и перехват		
	Осуществляется контроль жизненного цикла учетных записей работников		
	Ведется учет учетных записей тестовых пользователей, а также не персонифицированных учетных записей приложений и служб		
Антивирусная защита информации	Используется антивирусная защита средств обработки информации, контролируется актуальность антивирусных баз		
	Контролируется работоспособность антивирусного программного обеспечения, в т.ч. проводится его периодическое тестирование		
	Проводится антивирусная проверка всех файлов, полученных из внешних источников, и любых дистрибутивов программ, устанавливаемых на		

	устройства, обрабатывающие конфиденциальную информацию		
Защита информации при работе в сетях общего пользования	Используются средства межсетевого экранирования		
	Установлен запрет на работу в сетях общего пользования при отключенных средствах защиты информации		
	При передаче конфиденциальной информации через сети общего пользования используются методы и средства ее криптографической защиты, производится контроль актуальности и безопасности криптографических ключей		
	Установлен запрет на хранение конфиденциальной информации на не корпоративных облачных хранилищах		
	При удаленной работе с конфиденциальной информацией обеспечивается безопасность сетевых соединений к автоматизированным рабочим местам и серверам с использованием криптографических методов и технологии VPN		
Меры по обеспечению физической безопасности	Перенос конфиденциальной информации на материальные носители разрешен в исключительных случаях		
	Обеспечивается контроль физического доступа в помещения, в которых располагаются средства обработки и материальные носители конфиденциальной информации		
	Применяются средства противопожарной безопасности, резервного копирования данных, резервирования источников питания автоматизированных рабочих мест и серверов		
	Обеспечивается гарантированное уничтожение информации на материальных носителях информации после окончания ее обработки или в случаях выхода из строя компонентов средств обработки информации		
Реагирование на инциденты информационной безопасности	Производится регистрация событий информационной безопасности и их анализ		
	Производится обнаружение и регистрация инцидентов информационной безопасности, а так же реагирование на них		
	Организовано уведомление заинтересованных сторон об инцидентах информационной безопасности и причинах и условиях		

	их возникновения		
	Установлен запрет на разглашение информации об инцидентах информационной безопасности, без согласования всех заинтересованных сторон, кроме случаев, предусмотренных законодательством		
Организационные меры	Определено лицо, отвечающее за информационную безопасность		
	Утверждены и соблюдаются задокументированные политики, стандарты и регламенты, качающие вопросов информационной безопасности		
	Проводятся мероприятия по повышению осведомленности работников в области информационной безопасности, в том числе по вопросам противодействия фишингу и социальной инженерии		
	Ведется учет и контроль процедур обработки конфиденциальной информации		
	Обеспечивается подписание работниками обязательств о неразглашении сведений конфиденциального характера и соблюдения требований информационной безопасности		
Безопасная разработка ПО (в случае предоставления услуг, связанных с программными продуктами собственной разработки)	Обеспечивается безопасное проектирование, разработка, тестирование, поставка и сопровождение программных продуктов		
	Внедрены процессы безопасной разработки (желательно наличие формализованной политики)		
	Проводятся обязательные проверки безопасности (статический анализ кода, анализ сторонних компонентов, проверка на жёстко заданные конфиденциальные данные)		
	Устраняются выявленные уязвимости		
	Ведется статистика по количеству уязвимостей с уровнем критичности «Критический» и «Высокий» на каждом этапе анализа.		

Результат проведения контроля[2]:

☐	Технические и организационные меры обеспечения информационной безопасности, реализованные Организацией, **соответствуют** требованиям Стандарта по обеспечению информационной безопасности при информационном взаимодействии с контрагентами.

[2] Необходимо выбрать только **один** вариант результата проведения контроля.

☐	Технические и организационные меры обеспечения информационной безопасности, реализованные Организацией, **не в полной мере соответствуют** требованиям Стандарта по обеспечению информационной безопасности при информационном взаимодействии с контрагентами, но не противоречат требованиям законодательства Российской Федерации.
☐	Технические и организационные меры обеспечения информационной безопасности, реализованные Организацией, **не соответствуют** требованиям Стандарта по обеспечению информационной безопасности при информационном взаимодействии с контрагентами.

----------(конец формы)----------