

ТРЕБОВАНИЯ СІТІ К ПОСТАВЩИКАМ

ОТВЕТСТВЕННЫЕ:

Глава отдела Procurement & Risk в Citi

ДАТА ВЫПУСКА:

Январь 2015 г.

РЕДАКЦИЯ:

Сентябрь 2026 г.

ВЕРСИЯ:

9

СОДЕРЖАНИЕ

1	ОБЩИЙ ОБЗОР	3
2	РАВНЫЕ ВОЗМОЖНОСТИ ТРУДОУСТРОЙСТВА.....	5
3	ПРОТИВОДЕЙСТВИЕ ВЗЯТОЧНИЧЕСТВУ И КОРРУПЦИИ (AB&C).....	7
4	ПОДАРКИ И ПРЕДСТАВИТЕЛЬСКИЕ РАСХОДЫ.....	7
5	ВЗАИМОДЕЙСТВИЕ С ПОСТАВЩИКАМИ И ПРИНЦИПЫ ВЗАИМОДЕЙСТВИЯ С ПОСТАВЩИКАМИ	8
6	ЗАПРЕТ НА СОВРЕМЕННОЕ РАБСТВО	8
7	ПЕРСОНАЛ ПОСТАВЩИКА	11
8	ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ	12
9	ВЗАИМОДЕЙСТВИЕ СО СМИ И ПУБЛИЧНЫЕ ВЫСТУПЛЕНИЯ.....	15
10	ПИСЬМЕННЫЕ ЭЛЕКТРОННЫЕ КОММУНИКАЦИИ.....	15
11	ПОЛИТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ И ВЗНОСЫ НА ПОЛИТИЧЕСКИЕ ЦЕЛИ 16	
12	ПРОТИВОДЕЙСТВИЕ ОТМЫВАНИЮ ДЕНЕЖНЫХ СРЕДСТВ (AML).....	17
13	УПРАВЛЕНИЕ ДОКУМЕНТАМИ	19
14	УСТОЙЧИВОСТЬ / НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ.....	21
15	МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ПРОВЕРКИ АНКЕТНЫХ ДАННЫХ.....	28
16	РАСХОДЫ	31
17	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ)	32
18	РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НА РАБОЧЕМ МЕСТЕ	76
19	ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ (ВКЛЮЧАЯ ГЕНЕРАТИВНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И АГЕНТНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ)	77
20	ЖАЛОБЫ КЛИЕНТОВ	79
21	ПОЛИТИКА В ОТНОШЕНИИ ЛИЧНОЙ ТОРГОВЛИ И ИНВЕСТИЦИЙ	80
22	СТАНДАРТЫ ВЫСТАВЛЕНИЯ СЧЕТОВ.....	80
23	ПОЛИТИКА ОБЯЗАТЕЛЬНОГО ОТСУТСТВИЯ НА РАБОЧЕМ МЕСТЕ	81
	ПРИЛОЖЕНИЕ — ОПРЕДЕЛЕНИЯ	82

1 ОБЩИЙ ОБЗОР

1.1. Общие требования

В настоящих Требованиях Citi к поставщикам (далее — «**Требования**») подробно описаны некоторые обязательства, которые Поставщики должны выполнять в ходе ведения бизнеса с Citi. Некоторые Требования применимы ко всем Поставщикам, в то время как применимость других Требований к конкретному Поставщику зависит от типов продуктов и услуг, которые Поставщик предоставляет Citi (последние кратко описаны ниже в Разделе 1.2 и приведены в начале каждого его положения). Термины, написанные с заглавной буквы, имеют значения, определенные для них в тексте настоящего документа, в том числе в прилагаемом Приложении, за исключением случаев, когда такое значение не указано в тексте настоящего документа (в таком случае они употребляются в значении, указанном для них в Договоре, как определено ниже).

Настоящие Требования являются договорными обязательствами по соглашениям Поставщиков с Citi (включая, помимо прочего, документы, относящиеся к сделке, а именно рабочие наряды, графики лицензий и т. д.) (каждое из которых именуется «**Договор**») и дополняют любые обязательства, указанные в любом Соглашении, любые обязательства в соответствии с Применимым законодательством (согласно данному ниже определению этого термина), любое уведомление Поставщику от Citi, информирующее Поставщика о его обязательствах в соответствии с ним (каждое из которых именуется «**Уведомление**»), или любые дополнительные более конкретные требования, предъявляемые бизнес-структурами или функциональными подразделениями Citi. В случае возникновения противоречий между любым из вышеперечисленных и настоящих требований применяются более ограничительные обязательства и требования. Поставщики должны проявлять активную позицию и консультироваться со своим основным контактным лицом в Citi (или назначенным лицом) по любым вопросам, возникающим у них в отношении настоящих Требований, включая любые изменения в них, любое запрошенное освобождение от их соблюдения или любое предполагаемое противоречие в них или с Применимым законодательством.

Поставщик должен незамедлительно выполнять любые обоснованные запросы, которые Citi может выдвинуть Поставщику относительно данных, необходимых Citi в рамках предоставления услуг поставщиков или персонала в связи с обязательством Citi соблюдать Применимое законодательство. Несоблюдение Поставщиком этих обязательств считается существенным нарушением условий настоящего Соглашения.

Несоблюдение настоящих Требований или любых дополнительных требований, установленных подразделением Citi, с которым Поставщик ведет дела, может привести к расторжению Договора Поставщика с Citi. Более того, нарушение Требований также может являться нарушением применимого законодательства и привести в порядке гражданского судопроизводства к взысканию убытков в пользу Citi (или третьих сторон), либо к привлечению поставщика к уголовной ответственности. Поставщик не имеет права использовать соблюдение своих собственных политик в качестве замены своих обязательств по соблюдению каких-либо положений настоящих Требований без письменного согласия Citi.

1.2. Требования, применимые к отдельным поставщикам

В следующей таблице перечислены некоторые Требования, которые применяются к определенным Поставщикам, отвечающим указанным в настоящем документе критериям применимости. Разделы, не упомянутые ниже, применимы ко ВСЕМ поставщикам.

Номер раздела	Название раздела	Применимость
2	РАВНЫЕ ВОЗМОЖНОСТИ ТРУДОУСТРОЙСТВА / ПОЗИТИВНЫЕ ДЕЙСТВИЯ	Применимо к договорам и заказам на покупку, необходимым для выполнения договора Citi с федеральным правительством США; если существует неопределенность в отношении того, является ли договор или заказ на покупку субподрядом или заказом на покупку федерального правительства, укажите «По мере необходимости» в начале или конце положения в зависимости от ситуации.
12	БОРЬБА С ОТМЫВАНИЕМ ДЕНЕГ	Применимо к Поставщикам, выполняющим определенные услуги, связанные с клиентами (т. е. прием клиентов на обслуживание, проверка клиентских счетов и транзакций), или предоставляющим данные или параметры, связанные с указанными выше действиями; <u>И (ИЛИ)</u> к ситуациям, когда Поставщик выступает в качестве посредника в отношении денежных средств или финансовых инструментов (напр., дистанционная обработка расчетов чеками, услуги курьера, предоставление бронированного автомобиля или сейфа).
13	УПРАВЛЕНИЕ ДОКУМЕНТАМИ	Применимо к Поставщикам, имеющим доступ к информации Citi, обрабатывающим или хранящим информацию Citi
14	НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ	Применимо к Поставщикам, предоставляющим услуги или размещающим технологическую инфраструктуру или приложения, используемые Citi. Специалист, отвечающий за деятельность бизнес-структуры Citi (BAO), несет ответственность за информирование поставщика о применимости и требованиях в отношении непрерывности деятельности.
15	МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ПРОВЕРКИ АНКЕТНЫХ ДАННЫХ	Применимо к Поставщикам, предоставляющим услуги для компании Citi.
16	РАСХОДЫ	Применимо к Поставщикам, которые по договору вправе требовать возмещения деловых расходов.

Номер раздела	Название раздела	Применимость
17	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ)	Применимо к Поставщикам, включая Субподрядчиков, которые получают доступ к информации Citi, обрабатывают такую информацию, управляют ею или хранят ее; <u>И (ИЛИ)</u> Поставщикам, ответственным за хостинг интернет-приложений под брендом Citi; <u>И/ИЛИ</u> Поставщикам с возможностью подключения к сетевым ресурсам Citi; <u>И/ИЛИ</u> Поставщикам, которым требуется доступ на объекты Citi без сопровождения.
18	РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НА РАБОЧЕМ МЕСТЕ	
19	ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ (включая генеративный искусственный интеллект и агентный искусственный интеллект)	Применимо к Поставщикам, которые используют искусственный интеллект или машинное обучение (AI/ML), в соответствии с определением Citi, в любой части продукта или услуги, которые они предоставляют.
20	ПОЛИТИКА В ОТНОШЕНИИ ЛИЧНОЙ ТОРГОВЛИ И ИНВЕСТИЦИЙ	Применимо к Поставщикам, которым требуется регулярный доступ к информации MNPI в рамках своих должностных обязанностей в Citi.
23	ПОЛИТИКА ОБЯЗАТЕЛЬНОГО ОТСУТСТВИЯ НА РАБОЧЕМ МЕСТЕ	Данная политика применима к лицам, не являющимся сотрудниками («Работники»), которые занимают особо ответственные должности (как определено в Глоссарии) («Работники, занимающие особо ответственные должности»), а также непосредственные руководители и супервайзеры сотрудников, занимающих ответственные должности («Руководители»), и контактные лица бизнес-структур Citi для сотрудников, занимающих ответственные должности.

2 РАВНЫЕ ВОЗМОЖНОСТИ ТРУДОУСТРОЙСТВА

2.1 Равные возможности трудоустройства

Citi разработала политики, которые призваны обеспечить равные возможности трудоустройства для всех соответствующих лиц независимо от расы, цвета кожи, религии, пола, сексуальной ориентации, гендерной идентичности, национального происхождения, возраста, семейного положения, генетической информации, инвалидности, защищенного статуса ветерана или любого другого фактора, дискриминация по которому запрещена законом.

Поставщики должны соблюдать и обеспечивать соблюдение своим персоналом требований всех применимых законов и нормативных актов о недопущении дискриминации, включая, помимо прочего, любые законы или нормативные акты, относительно необходимости соблюдения которых Citi уведомляет Поставщика в письменной форме.

Поставщики должны изучить Заявление Citi о политике обеспечения равных возможностей трудоустройства в США и принять соответствующие меры в соответствии с ним. Заявление можно найти на сайте

www.citigroup.com/global/eeo-aa-policy.

2.2 Государственные контракты

В контрактах и заказах на закупку, необходимых для исполнения контракта Citi с федеральным правительством, должно быть дословно воспроизведено напечатанное жирным шрифтом следующее положение, как показано ниже. (Если неясно, идет ли речь о субподряде/заказе на закупку с участием федерального правительства, допустите, что необходимо добавить слова «По мере необходимости» в начало раздела).

[По мере необходимости] Поставщик обязуется соблюдать все применимые федеральные законы о борьбе с дискриминацией и заверяет, что не реализует никаких программ в нарушение применимых федеральных законов о борьбе с дискриминацией.

2.3 Приложение о государственных контрактах

Договоры и заказы на закупку, необходимые для исполнения контракта Citi с федеральным правительством, должны содержать следующее уведомление в приложении к субподряду или заказу на закупку. (Если неясно, идет ли речь о субподряде/заказе на закупку с участием федерального правительства, допустите, что необходимо добавить слова «По мере необходимости» в конце уведомления ниже.)

Как подрядчик федерального правительства, Citigroup настоящим предоставляет нижеподписавшемуся подрядчику или поставщику письменное уведомление о наших обязательствах в отношении равных возможностей трудоустройства в интересах защищенных ветеранов и инвалидов. Citigroup в полной мере исполняет раздел 503 Закона о реабилитации и Закона о содействии социальной реинтеграции ветеранов войны во Вьетнаме, а также его применимых нормативных актов согласно § 60-741 § 60-300 § 41 C.F.R. соответственно. Наше Заявление о политике обеспечения равных возможностей трудоустройства можно найти на сайте www.citigroup.com/global/eeo-aa-policy. Все вопросы о нашем Заявлении о политике ЕЕО можно направлять контактному лицу, указанному в нашем Заявлении о политике.

[По мере необходимости] Мы просим вас принять соответствующие меры в соответствии с нашим Заявлением о политике и нормативными актами.

3 ПРОТИВОДЕЙСТВИЕ ВЗЯТОЧНИЧЕСТВУ И КОРРУПЦИИ (AB&C)

Citi разработала разумные политики, процедуры и средства внутреннего контроля в целях соблюдения применимых законов об AB&C и строго запрещает взяточничество и предоставление платежей за упрощение формальностей в любом виде. Поставщики (включая коммерческих инициаторов), их Персонал или любые лица, прямо или косвенно действующие от имени Citi, обязуются осуществлять свою деятельность в соответствии с самыми высокими этическими стандартами и в соответствии с Законом США о коррупции за рубежом (FCPA), Законом Великобритании о взяточничестве (UKBA) в их актуальной редакции и всеми другими применимыми местными законами об AB&C тех стран, в которых работает Citi.

Всем Поставщикам и их Персоналу, действующему от имени Citi или в связи с любыми соглашениями или взаимоотношениями Поставщика с Citi, запрещается (i) совершать, предоставлять, авторизовывать или предлагать любые платежи, бонусы, преимущества или любые другие ценности какому-либо лицу; и (ii) получать или принимать какие-либо платежи, бонусы, преимущества или любые другие ценности от любого лица в случаях (i)-(ii) в нарушение FCPA, UKBA или любых других законов об AB&C. Поставщик и его Персонал должны осуществлять свою деятельность и транзакции от имени Citi или в связи с любым из соглашений Поставщика или взаимоотношений с Citi в соответствии с Требованиями, включая данный раздел. Поставщик и его Персонал также должны реализовать программу соблюдения AB&C, а также политики и процедуры, разработанные и применяемые для обеспечения соблюдения всех законов об AB&C.

Для ознакомления с программой Citi по AB&C посетите веб-страницу [Citigroup's Investor Relations](#) (в разделе «Политики Citi» выберите «AB&C Program»).

4. ПОДАРКИ И ПРЕДСТАВИТЕЛЬСКИЕ РАСХОДЫ

Поставщики и их Персонал не имеют права предоставлять сотрудникам Citi подарки и любые ценности (включая приглашения на развлекательные мероприятия), если это создает фактический или видимый конфликт интересов, взаимовыгодный обмен, способно поставить под вопрос добросовестность или объективность решений сотрудника или иным образом негативно повлиять на его решения или заставить сотрудника действовать вразрез со своими обязанностями или иным образом нарушать применимое законодательство. Не ограничивая вышеизложенное, сотрудник должен придерживаться раздела «Запрещенные подарки и развлечения» стандарта G&E. Поставщики и их Персонал не должны предоставлять сотрудникам Citi безналичные бизнес-подарки совокупной стоимостью более 300 долларов США на человека в календарный год.

Если Поставщик предлагает сотруднику Citi деловое развлекательное мероприятие (приглашение на обед, спортивное, культурное или аналогичное мероприятие), Поставщик должен сам присутствовать на мероприятии, а мероприятие должно быть подходящим случаю, общепринятым и обоснованным, не чрезмерно роскошным или слишком регулярным. Более того, если Поставщик не присутствует на мероприятии, развлечения считаются деловым подарком и должны соответствовать применимым пороговым значениям отчетности, установленным в Стандарте для подарков и развлечений Citi. Поставщику запрещается от имени Citi или предположительно от имени Citi предоставлять какие-либо ценности, в том числе за счет самого Поставщика или сотрудника Citi, прямо или косвенно, каким-либо лицам или побуждать другое лицо выполнить вышеуказанные действия, если это будет или может быть обоснованно воспринято как коррупционное или неуместное действие, либо действие, нарушающее применимое законодательство.

5 ВЗАИМОДЕЙСТВИЕ С ПОСТАВЩИКАМИ И ПРИНЦИПЫ ВЗАИМОДЕЙСТВИЯ С ПОСТАВЩИКАМИ

<https://www.citigroup.com/citi/suppliers/> Citi взаимодействует с поставщиками в рамках ряда инициатив и повышает осведомленность о программе закупок Citi среди потенциальных поставщиков из сообществ, в которых мы осуществляем свою деятельность. Кроме того, такое взаимодействие направлено на выявление потенциальных поставщиков, в особенности поставщиков, использующих передовые решения для решения возникающих проблем, связанных с коммерческой деятельностью. С дополнительной информацией о требованиях Citi в отношении поставщиков можно ознакомиться на странице [Doing Business with Citi](#):

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 ЗАПРЕТ НА СОВРЕМЕННОЕ РАБСТВО

Citi стремится поддерживать методы, направленные на выявление и устранение рисков современного рабства и торговли людьми, которые могут возникать внутри организации или цепочек поставок. Поставщики Citi должны соблюдать изложенные ниже Требования и разрабатывать эффективные общекорпоративные политики, процедуры и/или методы для выявления и устранения рисков современного рабства и торговли людьми в рамках своих собственных операций и цепочек поставок. Поставщики по запросу Citi обязуются заполнить Анкету Citi о корпоративной ответственности, включив в нее всю необходимую дополнительную информацию, чтобы позволить Citi оценить подверженность риску и возможные меры по его снижению, особенно для Поставщиков в отраслях и регионах с повышенным риском. Субподрядчики Поставщика должны соблюдать такой же процесс.

6.1 Отказ от использования детского труда

Требования Citi к поставщикам

Поставщики не должны использовать детский труд. Термин «ребенок» относится к любому лицу, не достигшему минимального возраста трудоустройства в соответствии с применимыми законами, или, в случае отсутствия таких законов, к любому лицу возрастом до 15 лет или до возраста завершения обязательного образования, в зависимости от того, какой из этих возрастов больше. При условии соблюдения приоритетного запрета на использование детского труда, если на работу принимаются работники в возрасте до 18 лет, особое внимание следует уделять выполняемым ими обязанностям и условиям, в которых им приходится работать, чтобы гарантировать, что им не будет причинен физический, психический или иной вред как прямой или косвенный результат их работы или условий труда.

6.2 Трудоустройство по принципу свободного выбора

Поставщик должен обеспечить, чтобы работники не подвергались принуждению, умственному или физическому давлению, рабскому, кабальному труду или недобровольному труду в тюрьмах, работоторговле или любой форме принудительного труда, включая принудительные сверхурочные. Работник должен выполнять всю работу добровольно. Обязательства Поставщика в соответствии с настоящим документом, должны предусматривать, помимо прочего, соблюдение следующих требований.

- 1. Договоры, заработная плата и продолжительность рабочего времени.** Условия занятости или участия трудящихся должны быть изложены в письменном документе, который понятен трудящимся и четко определяет их права и обязанности. Такой письменный документ должен включать в себя, помимо прочего, прозрачные условия в отношении заработной платы, оплаты сверхурочной работы, периодов оплаты труда, рабочего времени и прав в отношении перерывов для отдыха и отпусков. Такие письменные условия должны быть предоставлены работнику до начала его работы у работодателя, должны соблюдаться работодателем и должны соответствовать отраслевым стандартам и минимальным требованиям применимых законов и коллективных договоров по месту выполнения работы.
- 2. Право свободно прерывать трудовые отношения.** Трудящиеся должны иметь право свободно прерывать трудовые отношения, по мере необходимости, по истечении разумного периода уведомления в соответствии с применимыми законами и коллективными договорами и без каких-либо неправомерных наказаний.
- 3. Бесчеловечное обращение.** Работники, их семьи и лица, тесно связанные с ними, не должны подвергаться жестокому или бесчеловечному обращению, включая, помимо прочего, физическое наказание, физическое, психологическое или сексуальное насилие или принуждение, словесные оскорбления, домогательства и запугивание. Трудящиеся-мигранты, их семьи и лица, тесно связанные с ними, не должны подвергаться дискриминации в отношении условий труда по признаку своей национальной принадлежности.

4. **Заработная плата, пособия и продолжительность рабочего времени.** Вознаграждение должно соответствовать всем применимым законам о заработной плате, включая законы, касающиеся минимальной заработной платы, сверхурочного времени и предусмотренных законом пособий. Сотрудникам следует выплачивать заработную плату в полном объеме и своевременно, а в расчетных листках вся информация о заработной плате должна быть указана четко и понятно. В качестве меры дисциплинарного воздействия не должны применяться никакие штрафные вычеты или удержания заработной платы или выплат. Длительность рабочей недели не должна превышать максимальной длительности, установленной местным законодательством. Сверхурочная работа должна выполняться добровольно в пределах установленных законом ограничений, а за отказ от нее сотрудник не должен быть наказан.
5. **Запрет на конфискацию документов, удостоверяющих личность.** У работников нельзя конфисковывать и удерживать удостоверение личности, разрешение на поездку, паспорт и другие официальные документы или любые другие ценные вещи в качестве условия приема на работу, а удержание имущества не должно использоваться прямо или косвенно для ограничения свобод работников и создания рабства на рабочем месте.
6. **Запрет на оплату работниками сборов и расходов при трудоустройстве или долговая кабала.** Работники не должны ни прямо, ни косвенно оплачивать сборы и расходы, связанные с наймом работников (включая, помимо прочего, сборы за предоставление рабочей визы, транспортные расходы и расходы на обработку документов). Аналогичным образом, трудящиеся не обязаны производить платежи, имеющие целью или следствием создание ситуации рабства на рабочем месте, включая выплаты за обеспечение безопасности, а также не должны выплачивать долги в форме труда. Если будет определено, что с работников были взысканы комиссии или сборы в рамках процесса найма на работу или если такие комиссии или сборы были понесены во время трудоустройства, Поставщик должен принять обоснованные меры, чтобы немедленно возместить такие затраты. При необходимости привлечения работников посредством третьих сторон, таких как агентства по подбору персонала, следует выбирать только надежные агентства по подбору персонала. В случае прямого найма работников следует пользоваться услугами только кадровых агентств с хорошей репутацией. Запрет взимать плату с работника за его трудоустройство распространяется на всех сотрудников кадровых агентств, агентов и субагентов. Поставщики должны иметь средства контроля, позволяющие обеспечить соблюдение этих требований. **Свобода передвижения.** Работники должны иметь возможность свободно передвигаться без необоснованных ограничений, и их передвижение не должно быть физически ограничено местом работы

или другими контролируруемыми работодателем местами (например, местом проживания работника). Трудящиеся не обязаны размещаться в контролируемых работодателем помещениях, за исключением случаев, когда это необходимо в силу расположения или характера выполняемой работы.

7. Возможность подавать жалобы, не опасаясь преследования.

Работникам должно быть предоставлено право подавать жалобы на работодателя в случае несправедливого обращения с ними; при этом жалобы не должны караться никакими ответными репрессивными мерами, приводить к причинению вреда или ответным обвинениям.

7 ПЕРСОНАЛ ПОСТАВЩИКА

7.1 Обучение Персонала Поставщика, назначение, переназначение и управление

Поставщик обязуется использовать достаточное количество лиц с соответствующей подготовкой, образованием, опытом и навыками для предоставления Услуг по Договору наиболее эффективным образом и обязуется по запросу подтвердить квалификацию таких лиц. После назначения Персонала для участия в Проекте Поставщик не будет переназначать или использовать Персонал для других целей, которые снижают доступность Персонала для работы над Проектом, без предварительного письменного согласия Citi, и, как правило, Поставщик будет назначать Персонал для участия в Проектах таким образом, чтобы свести к минимуму простои, связанные с необходимостью переподготовки Персонала. Поставщик должен следить за тем, чтобы его Персонал не позиционировал себя как сотрудников или представителей Citi и не стремился к тому, чтобы с ним обращались как с сотрудниками Citi в каких-либо целях, в том числе с целью использовать право на дополнительные льготы, предоставляемые Citi, или на получение доходов по нетрудоспособности, уплату налогов по программе социального страхования, получение пособий по социальному обеспечению, уплату федеральных налогов в фонд пособий по безработице, получение пособий в рамках страхования по безработице или удержание федерального подоходного налога. Поставщик несет единоличную ответственность за все обязанности работодателя в отношении своего Персонала, в том числе, помимо прочего, за наличие всех необходимых страховых покрытий, подачу всех применимых налоговых деклараций и уплату всех необходимых платежей и налогов в порядке, соответствующем статусу Поставщика как независимого подрядчика.

7.2 Замена Персонала Поставщика

Поставщик обязуется отстранить и заменить Персонал, назначенный Поставщиком для участия в Проекте, если Citi уведомит Поставщика о том, что Персонал неприемлем для Citi по любой причине, не предполагающей дискриминации. Поставщик также соглашается отстранить и заменить Персонал, назначенный для участия в Проекте, и немедленно запретить ему предоставлять Услуги Citi (или брать на себя любую ответственность в отношении предоставления Услуг или надзора

за ними), если Персонал не может или не желает предоставлять Услуги своевременно и профессионально.

7.3 Кадровая политика Поставщика

Поставщик заявляет, гарантирует и обязуется соблюдать и эффективно применять комплексные политики и процедуры для квалификационной оценки своего Персонала, являющегося физическими лицами, которому поручено предоставлять Citi Услуги на месте, а также заявляет и гарантирует, что эти политики и процедуры включают в себя проверку разрешений на работу, проверку биографических данных о трудовой деятельности и проверку на наличие судимостей, как указано далее в настоящем документе, а также проверку на предмет употребления наркотиков перед приемом на работу. Все вышеописанное осуществляется в той мере, в какой это разрешено применимым законодательством и любым применимым коллективным договором. Не ограничивая общего характера вышеизложенного, Поставщик также заявляет, гарантирует и обязуется, что у него есть средства контроля и процедуры для обеспечения полного соблюдения Поставщиком всех иммиграционных Применимых законов, включая подтверждение того, что весь Персонал Поставщика, назначенный для взаимодействия с Citi, уполномочен работать на протяжении всего задания в полном соответствии со всеми иммиграционными Применимыми законами. По запросу Поставщик незамедлительно предоставит Citi письменное подтверждение разрешения на работу для любого или всего Персонала Поставщика, назначенного для взаимодействия с Citi, и его соответствия иммиграционному Применимому законодательству, а также заменит любой Персонал, не имеющий разрешения на работу в соответствии с Применимым законодательством, на соответствующим образом квалифицированный Персонал, включая предоставление всего необходимого обучения и инструктажа для обеспечения своевременного и эффективного предоставления Услуг, не требуя дополнительной оплаты от Citi.

7.4 Владельцы Поставщиков

Для соблюдения применимых законов и нормативных актов в юрисдикциях, в которых Citi ведет бизнес, по запросу Citi поставщики обязаны предоставлять данные о владельцах, являющихся физическим лицом и/или организацией, включая непосредственного владельца (владельцев) поставщика, вплоть до и включая конечного бенефициарного владельца, имеющего право собственности или контроля прямо или косвенно через влияние или другие средства на участие, продукт или услугу.

8 ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ

В рамках деятельности Citi по выявлению и снижению риска мошенничества («Противодействие мошенничеству»).

8.1 Все поставщики должны:

1. Оказывать содействие при расследованиях Citi случаев предполагаемого воровства, мошенничества и другой потенциальной преступной деятельности или правонарушений, а также при любых

судебных преследованиях мошеннического или преступного поведения в полном объеме, предусмотренном законом.

2. Своевременно сообщать и передавать в Citi информацию о случаях потенциального мошенничества через [Ethics Hotline](#); помимо прочего, сюда относятся попытки, подозрения, обвинения и факты воровства и мошенничества (например, предоставление заведомо ложной, неверной или искаженной информации относительно поставщика, схем биллинга, исчезновение денежных средств или ценных бумаг и т. д.), преступная деятельность и правонарушения, затрагивающие Citi, сотрудника, поставщика или агента Citi, а также лиц, не являющихся сотрудниками Citi (например, временных сотрудников или субподрядчиков).
3. Позволять Citi и ее представителям осуществлять мониторинг и надзор и оказывать содействие расследованиям, проводимым Citi и правоохранительными органами в отношении потенциально мошеннических действий, касающихся данного Поставщика.
4. Своевременно сообщать о любых конфликтах интересов (включая конфликты интересов между Поставщиками/Сотрудниками поставщиков и/или Сотрудниками Citi), о которых становится известно Поставщикам.
5. Поддерживать процессы Citi по предотвращению мошенничества во время настройки или обновления банковского счета Поставщика в платежной системе Поставщика Citi.

8.2 Кроме того, Поставщики, оказывающие услуги, в силу своего характера более уязвимые для мошенничества, **обязаны** выполнять следующие действия:

1. Документально фиксировать и выполнять программу управления рисками мошенничества, выявляющую существенные риски мошенничества, связанные с услугами, предоставляемыми Citi, а также средства контроля и процедуры, предусмотренные для уменьшения этих рисков.
2. Пройти обучение по вопросам борьбы с мошенничеством (в течение 90 календарных дней после приема на работу и затем ежегодно) и обучить персонал конкретным элементам риска мошенничества, связанным с конкретными услугами, предоставляемыми Citi.
3. Отслеживать случаи попыток мошенничества и поддерживать эффективные средства контроля в целях уменьшения риска мошенничества в отношении услуг, предоставляемых Citi, документально фиксировать процедуры использования средств контроля и проверять эффективность средств контроля на постоянной основе, сообщая обо всех недостатках специалисту, отвечающему за деятельность подразделения (BAO).
4. Предоставлять любую необходимую информацию для проверки на благонадежность/постоянного мониторинга/оценки риска мошенничества специалисту, отвечающему за деятельность бизнес-структуры (BAO).

5. Проверка на благонадежность включает в себя Шаблон оценки воздействия мошенничества на третьих лиц (TP-FIAT), который предназначен для проведения контрольных оценок возможностей Поставщиков в отношении снижения рисков мошенничества. Эта рабочая процедура описывает ряд шагов, которые должны быть выполнены специалистом, отвечающим за деятельность бизнес-структуры (BAO), или сотрудником третьей стороны (ТРО) и сотрудником по управлению рисками мошенничества (FRMO) для выявления рисков мошенничества и управления ими.

8.3 К поставщикам, для которых характерен более высокий риск мошенничества, относятся, помимо прочего, лица, которые:

1. имеют доступ к данным, классифицированным как конфиденциальные или имеющие более высокий уровень защиты (когда такие данные не находятся под прямым контролем или надзором Citi), которые могут использоваться для содействия мошенничеству, например, для доступа к служебным счетам, финансовым операциям и операциям с наличными;
2. подключены к сетям или системам Citi; и
3. предоставляют услуги и возможности, которые могут стать целями мошенников, поддерживают такие услуги и возможности или имеют доступ к ним, включая следующие услуги и возможности:
 - a) выявление, прием и обработка заявок от новых клиентов;
 - b) операции Citi или клиентов, связанные с платежами или денежными переводами и (или) подтверждение подлинности клиентов Citi, осуществляющих доступ к этим услугам;
 - c) разработка, проверка и внесение изменений в данные Citi или клиента Citi (например, демографические данные);
 - d) предоставление, обслуживание или авторизация транзакционных инструментов (например, дебетовых или кредитных карт, электронных кошельков, чековых книжек и т. д.);
 - e) предоставление Citi или поддержка операционных мер по противодействию мошенничеству, связанных с предотвращением, выявлением и реагированием на случаи мошенничества;
 - f) предоставление физического доступа к наличным деньгам, финансовым инструментам и активам или физическим товарам;
 - g) доступ на объекты Citi без сопровождения или в нерабочее время;
 - h) финансовая отчетность: бухгалтерские операции, такие как внесение записей в главную бухгалтерскую книгу (GL) и книгу регистрации продаж (SL);
 - i) получение и использование бонусов за поощряемые действия.

9 ВЗАИМОДЕЙСТВИЕ СО СМИ И ПУБЛИЧНЫЕ ВЫСТУПЛЕНИЯ

Citi Enterprise Services and Public Affairs — единственный отдел, уполномоченный выпускать пресс-релизы или делать публичные заявления от имени Citi. Поставщики не вправе выпускать пресс-релизы, прямо или косвенно упоминающие Citi, договора или соглашения между Поставщиком и Citi или продукты и услуги, предоставляемые Поставщиком Citi. Поставщикам запрещается соглашаться на участие и участвовать в любой деятельности по связям с общественностью, которая касается Citi и в которой также участвуют Клиенты, сотрудники Citi, другие Поставщики Citi, другие заказчики Поставщиков или прочие третьи стороны, без предварительного письменного разрешения их основного контактного лица в Citi.

Поставщики не вправе публиковать или размещать какие-либо материалы в письменном или электронном формате (включая книги, статьи, подкасты, веб-трансляции, блоги, публикации на веб-сайтах, фотографии, видео, социальные сети или другие медиа), произносить речи или выступать с заявлениями, давать интервью или совершать публичные выступления, в которых упоминается Citi, деятельность Citi, Клиенты, продукты или услуги, без предварительного письменного разрешения их основного контактного лица в Citi и старшего сотрудника по связям с общественностью в стране.

Независимо от того, связано ли это с предоставлением услуг или продуктов Citi, Поставщики не должны использовать принадлежащие Citi фирменные знаки, торговые знаки, знаки обслуживания, торговые наименования, логотипы, символы или названия брендов без получения в каждом случае предварительного письменного согласия от Citi. Поставщики не вправе использовать название, логотип или товарные знаки, объекты или связи Citi в интересах или для работы за пределами Citi (в том числе на фирменных бланках или личных веб-сайтах, в блогах или на других сайтах социальных сетей). Кроме того, Поставщикам запрещено использовать название, объекты и взаимоотношения Citi с целью проведения благотворительных или бесплатных мероприятий.

10 ПИСЬМЕННЫЕ ЭЛЕКТРОННЫЕ КОММУНИКАЦИИ

При взаимодействии с персоналом Citi или при выполнении своих обязательств для или от имени Citi, Поставщикам разрешается использовать только одобренное Citi оборудование, системы и услуги электронной связи. Новые, расширенные или модифицированные каналы связи Citi eComm, либо используемые как отдельные инструменты, либо интегрированные в более широкую платформу, предоставленные Citi или третьей стороной, подлежат утверждению в соответствии с применимыми Требованиями Citi, о которых Поставщик получил письменное уведомление от своего БАО. Запрещается обсуждение рабочих вопросов Citi с персоналом Citi на платформах обмена сообщениями, не одобренных Citi, таких как WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber и любые другие интерактивные электронные платформы.

Кроме того, Поставщикам не следует требовать конфиденциальности в отношении письменных электронных сообщений, которые создают, выявляют, используют, открывают, загружают, сохраняют, передают, получают и удаляют с помощью предоставляемых Citi коммуникационного оборудования, систем и услуг. Citi имеет право осуществлять мониторинг электронного коммуникационного оборудования, систем и услуг, а также электронной коммуникации. Подобные электронные коммуникации являются собственностью Citi и могут храниться в соответствии с применимыми требованиями к хранению документов (в соответствии с местным законодательством и нормативно-правовыми требованиями).

<https://policydirectory.citi.net/cpd/ layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 ПОЛИТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ И ВЗНОСЫ НА ПОЛИТИЧЕСКИЕ ЦЕЛИ

Разнообразные законы, например, такие, которые относятся к таким сферам, как иностранное влияние, финансирование политических кампаний, подарки и представительские расходы, законодательное лоббирование, лоббирование на низовом уровне, имиджевое лоббирование и регуляторное лоббирование, закупки, плата за доступ к услугам и ценные бумаги, регулируют политическую деятельность и разглашение информации, относящейся к такой деятельности, компании Citi и ее поставщиков. Любая политическая деятельность Поставщиков, которая не соответствует применимой политике или стандартам Citi, законодательству или нормативным актам, запрещена.

Политическая деятельность включает в себя, помимо прочего:

1. Внесение корпоративных или личных взносов на политические цели, просьбы о внесении взносов на политические цели, использование денежных средств или ресурсов компании (помещений, оборудования, программного обеспечения или персонала) или добровольное оказание помощи при проведении избирательной кампании, оказание услуг партийному или политическому комитету в рабочее время;
2. Лоббирование или оказание иных видов поддержки государственным должностным лицам (напрямую или через посредников), в том числе попытки повлиять на должностных лиц, законодательную деятельность и (в зависимости от юрисдикции) попытки повлиять на процесс разработки законодательства или госзакупок; либо
3. Попытки занять государственную должность или принятие государственной должности, в том числе в органах совета, комитетах или иных подобных государственных организациях.

Без предварительно полученного письменного разрешения отдела Government Affairs Global Operations Control (ggacontrol@citi.com) Поставщики не имеют права осуществлять политическую деятельность от имени (или предположительно от имени) Citi или ее клиентов. Хотя Citi может оплачивать сбор и/или возместить из собственных средств расходы на договорные и разрешенные услуги по политической деятельности, предоставляемые Поставщиком, такие как лоббирование, Citi никогда не возмещает Поставщику или его сотрудникам никакие личные или корпоративные расходы, связанные со взносами на любые политические цели.

12 ПРОТИВОДЕЙСТВИЕ ОТМЫВАНИЮ ДЕНЕЖНЫХ СРЕДСТВ (AML)

Применимо к Поставщикам, выполняющим определенные услуги, связанные с клиентами (т. е., прием клиентов на обслуживание, проверка клиентских счетов и транзакций) или предоставляющим данные или параметры, связанные с указанными выше действиями; И (ИЛИ) действующим в качестве посредника в отношении финансовых транзакций или инструментов (например, дистанционная обработка расчетов чеками, услуги курьера, предоставление бронированного автомобиля или сейфа, электронные переводы, цифровые активы).

12.1 Обязательства в сфере AML:

1. Соблюдение процессов Citi и применимых законов.

- Соблюдать и выполнять процессы и процедуры Citi, разработанные для соблюдения требований применимого законодательства, включая (i) Закон Грэмма — Лича — Блайли и изданные в соответствии с ним нормативно-правовые требования; (ii) Закон «Патриотический акт» США и изданные в соответствии с ним нормативно-правовые требования; (iii) любой закон или нормативно-правовое требование в сфере противодействия отмыванию денежных средств; и (iv) любой закон или нормативно-правовое требование в сфере экономических санкций. Такие политики и процедуры будут касаться ролей и обязанностей в сфере противодействия отмыванию денежных средств, включая требования о своевременном уведомлении о любой наблюдаемой активности, которая кажется необычной или вероятно необычной и связана с финансовой деятельностью, транзакциями и получением денежных средств.

2. Ежегодное обучение и элементы программы для персонала.

- Обеспечивать проведение ежегодного обучения Персонала, предоставляющего Услуги Citi, в отношении ролей и обязанностей в

сфере противодействия отмыванию денежных средств, включая требования о своевременном уведомлении о любой наблюдаемой активности, которая кажется необычной или вероятно необычной и связана с финансовой деятельностью, транзакциями и получением денежных средств. Обучение должно включать в себя, помимо прочего, следующие компоненты:

- а. Составление отчетов о подозрительной активности и эскалация вопросов, связанных с подозрительной активностью.
- б. Программа «Знай своего клиента» (KYC), включая программу идентификации клиентов (CIP), санкции и проверку имен, проверку клиентов на благонадежность (CDD), расширенную проверку на благонадежность (EDD), а также выявление и проверку **конечных бенефициаров (UBO)**.
- с. Мониторинг сделок в рамках всех соответствующих финансовых инструментов и действий.
- d. Периодическая отчетность/показатели, в том числе отчетность о юридических и регуляторных изменениях и существенных изменениях программ в сфере ПОД
- е. Проверка и контроль эффективности программы AML, включая посещение объектов.

3. **Соблюдение положений договора.**

- Соблюдать любые положения Договора, определяющие программу, которая должна быть внедрена Поставщиком.

4. **Незамедлительное предоставление уведомлений о предполагаемых нарушениях.**

- Незамедлительно сообщать Citi в письменном виде о любых предполагаемых нарушениях закона, в том числе о любой наблюдаемой активности, которая представляется необычной или вероятно необычной и связана с получением денежных средств, финансовой деятельностью или транзакциями, имеющими отношение к Citi или ее клиентам.

5. **Недопущение уклонения от уплаты налогов и уведомление об этом.**

- Обеспечить соблюдение всех применимых налоговых законов и нормативно-правовых требований в странах, в которых они осуществляют свою деятельность.

- Ни при каких обстоятельствах Поставщики не должны преднамеренно незаконно уклоняться от уплаты налогов или содействовать такому уклонению со стороны других лиц, что может включать участие в действиях, способствующих уклонению от уплаты причитающихся налогов или сокрытие информации от налоговых органов.
- Таким образом, Поставщики должны принять разумные меры по предотвращению уклонения от уплаты налогов и незамедлительно информировать Citi в письменном виде о любых нарушениях или предполагаемых нарушениях, имеющих отношение к Citi.

12.2 Внутренние политики и процедуры поставщика.

Поставщики должны соблюдать надлежащие внутренние политики и процедуры для соблюдения всех законов и нормативно-правовых требований в отношении AML, которые действуют сейчас или вступят в силу в будущем.

13 УПРАВЛЕНИЕ ДОКУМЕНТАМИ

Применимо к Поставщикам, имеющим доступ к информации Citi, обрабатывающим или хранящим информацию Citi

Citi требует, чтобы все Поставщики, обладающие информацией Citi, взаимодействовали со своим специалистом, отвечающим за деятельность бизнес-структуры («**BAO**»), или основным контактным лицом бизнес-структуры в Citi для (i) выявления и классификации информации как документов или временной информации в целях целей управления документами Citi, (ii) классификации документов в соответствии с каталогом основной документации Citi («**MRC**»), (iii) хранения информации в соответствии с требованиями по хранению Citi и (iv) при отсутствии требований о хранении информации надлежащим образом утилизировали информацию в конце жизненного цикла информации.

BAO или основное деловое контактное лицо Citi должны взаимодействовать с Поставщиком, чтобы гарантировать, что Поставщик выявляет и классифицирует документы в соответствии с кодами документов Citi в MRC, а Реестр обновляется не реже одного раза в год. Поставщик обязан соблюдать требования в отношении управления документами, установленные специалистом, отвечающим за деятельность бизнес-структуры (BAO). Документы, соответствующие критериям удаления, должны быть удалены надлежащим образом в максимально короткие сроки, но не позднее, чем через шесть месяцев после завершения выполнения требований по их хранению, за исключением случаев, когда их хранение регулируется требованиями в отношении хранения информации. Временную информацию, если на нее не распространяется требование о хранении, необходимо уничтожать не позже чем через два года после последнего

использования. Временные данные, включающие в себя персональные данные, должны быть удалены после того как будет достигнута цель, ради достижения которой их собирали, за исключением случаев, когда на них распространяется требование о хранении информации. Поставщик должен приостановить уничтожение или изменение информации Citi при получении уведомления о необходимости выполнять требование в отношении хранения информации. Поставщик обязан консультироваться с основным контактным лицом в Citi или с ВАО в случае сомнений.

Правила хранения документации, приведенные в графиках хранения документации по странам, ежеквартально проверяются и обновляются отделом DRIM по мере необходимости в соответствии с изменениями, внесенными в нормативно-правовые требования и внутренние политики. В случае внесения изменения, влияющего на Поставщика, специалист, отвечающий за деятельность бизнес-структуры, должен уведомить об этом Поставщика. Поставщик должен оценить влияние такого изменения и внести изменения в соответствующие системы, процессы и реестры. Поставщик должен внести изменения в документы, за которые он отвечает и которыми он управляет, в течение 90 дней с момента получения уведомления от специалиста, отвечающего за деятельность бизнес-структуры (ВАО).

Поставщики, ведущие документацию от имени Citi, несут ответственность за сохранение («хранение»), сбор и предоставление всей Информации, которая считается имеющей отношение к юридическому или иному разбирательству, в течение требуемого периода времени по запросу специалиста, отвечающего за деятельность бизнес-структуры (ВАО). Поставщик должен по запросу вернуть информацию компании Citi в соответствии с требованиями применимых договорных условий. Поставщикам запрещено уничтожать информацию Citi независимо от ее категории (например, конфиденциальная или неконфиденциальная) без разрешения основного контактного лица Citi или специалиста, отвечающего за деятельность бизнес-структуры (ВАО), в котором должно содержаться подтверждение, что в настоящий момент на информацию, подлежащую уничтожению, не распространяется требование о хранении информации. Требования к управлению документами и хранению документов и все другие требования в отношении обработки информации остаются в силе после расторжения или истечения срока действия Договора, если прямо не оговорено иное.

Поставщик должен вести письменный учет всего Персонала Поставщика, отвечающего за надзор за управлением информацией Citi, которая находится на хранении Поставщика, и периодически проводить совещания с основным контактным лицом бизнес-структуры Citi или должностным лицом, ответственным за управление документами, для проверки и изменения имен контактных лиц,

сведений о рабочих процедурах, ролей, обязанностей и журнала документации поставщика Citi.

14 УСТОЙЧИВОСТЬ / НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ

Применимо к Поставщикам, предоставляющим услуги или размещающим технологическую инфраструктуру или приложения, используемые Citi. Специалист, отвечающий за деятельность бизнес-структуры Citi (BAO), несет ответственность за информирование поставщика о применимости и требованиях в отношении непрерывности деятельности.

14.1 Аварийные ресурсы

План аварийного восстановления Поставщиков должен предоставлять альтернативные ресурсы, способные обеспечивать для Citi все продукты и услуги в том случае, если основные местоположения Поставщика окажутся недоступны. Аварийные ресурсы должны быть расположены в иных географических зонах, нежели основные ресурсы (на достаточном от них удалении), чтобы максимально снизить вероятность того, что чрезвычайное происшествие затронет обе зоны.

1. Под аварийными ресурсами понимаются не только информационные системы, а все ресурсы, необходимые для непрерывного предоставления продуктов или услуг Citi. Они могут включать персонал, здания, оборудование, центры обработки данных, вычислительные сети и сети передачи голосовых сообщений, транспортные услуги.
2. Поставщики приложений могут внедрить архитектуру типа Hot/Hot, чтобы обеспечить конфигурацию с высокой готовностью. Для такой архитектуры требуется наличие двух (как минимум) одинаково настроенных систем, которые запущены, работают и доступны клиентам (пользователям). Наиболее важной особенностью этой модели является то, что альтернативные среды работают одновременно с основным (производственным) центром обработки данных.

14.2 Уровни обслуживания при аварийном восстановлении

Для обеспечения эффективности работы Citi Поставщики должны соответствовать установленным уровням обслуживания. План аварийного восстановления Поставщика должен как минимум устанавливать конкретные значения для следующих параметров:

1. Целевое время восстановления
2. Целевая точка восстановления
3. Ресурсы восстановления / Технологический потенциал
4. Продолжительность восстановления

14.3 План аварийного восстановления

Поставщик обязуется поддерживать План аварийного восстановления для продолжения деятельности (и предоставлять доказательства своих текущих и периодических испытаний по запросу Citi), чтобы обеспечить способность

Поставщика незамедлительно предоставлять Продукты/Услуги и выполнять свои обязательства из другого места или с заменой Персонала, невзирая на любое нарушение способности Поставщика предоставлять Продукты/Услуги или выполнять свои другие обязательства по настоящему Соглашению из любого конкретного места или благодаря усилиям любых конкретных лиц. Копия Плана аварийного восстановления должна быть предоставлена Citi в течение десяти (10) календарных дней с Даты вступления в силу каждого Рабочего наряда, подписанного между Citi и Поставщиком, а затем ежегодно в течение срока действия каждого Рабочего наряда. Поставщик предоставит Citi инструкции или другую информацию, необходимую Citi для продолжения получения Продуктов/Услуг от Поставщика в обстоятельствах, когда Поставщик задействует свой План аварийного восстановления. Поставщик заявляет, гарантирует и обязуется, что его План аварийного восстановления будет включать в себя, как минимум, следующее:

1. процедуры и стратегии восстановления, включая переезд, передачу работы и/или удаленный доступ в целях смягчения последствий перебоев, включая недоступность технологий (отказ в обслуживании/DoS), недоступность основного места работы (отказ в доступе/DoA) и отсутствие персонала (включая субподрядчиков);
2. обслуживание Поставщиком, помимо прочего, вторичной площадки аварийного восстановления, отдельной от точек предоставления Продуктов/Услуг, хранение резервных носителей в месте, отдельном от точек предоставления Продуктов/Услуг, использование резервных линий связи и серверов;
3. процедуры резервного копирования/восстановления работы и применения Продуктов/Услуг, включая подробный, задокументированный план реагирования на продолжительные сбои в работе Продуктов/Услуг, вызванные сбоем питания, системным сбоем, стихийным бедствием или другими непредвиденными обстоятельствами, включая процессы и процедуры для возобновления деятельности в течение обоюдного согласованного периода времени;
4. процедуры защиты всего Контента;
5. процедуры и соглашения с третьими сторонами в отношении сменного оборудования (например, компьютерного оборудования);
6. процедуры для любых внеплощадочных производственных объектов; а также
7. план аварийного восстановления Поставщика будет предусматривать следующее:
 - a. Поставщик незамедлительно уведомляет Citi о любом стихийном бедствии, которое может негативно повлиять на Продукты/Услуги;
 - b. Поставщик предоставляет Citi в течение 24 часов с момента указанного уведомления план дальнейшего предоставления Продуктов/Услуг на альтернативном объекте;

- с. Продукты/Услуги должны предоставляться в полной мере в рамках требуемого целевого времени восстановления (RTO), которое, если в соответствующем договоре не указано иное, составляет 4 часа или менее для тех процессов, которым Citi присвоила категорию критичности Enterprise Critical или «ВЫСОКАЯ»; 24 часа или менее для тех процессов, которым Citi присвоила категорию критичности «СРЕДНЯЯ»; и 72 часа или менее для тех процессов, которым Citi присвоила категорию критичности «НИЗКАЯ»; а также
- d. если часть объектов Поставщика выйдет из строя, Поставщик будет обслуживать Citi на том же уровне, что и других коммерческих клиентов.

14.4 Требования к плану аварийного восстановления, применимые к Размещенным услугам

В тех случаях, когда Поставщик управляет Размещенной услугой Citi и предоставляет ее, также применяются следующие положения. План аварийного восстановления должен включать в себя как минимум следующее:

1. процедуры резервного копирования/восстановления работы и применения Размещенных сервисов, включая подробный документально оформленный план реагирования на продолжительные сбои в работе сервисов, вызванные сбоем питания, системным сбоем, стихийным бедствием или другими непредвиденными обстоятельствами, включая процессы и процедуры для возобновления деятельности в течение обоюдного согласованного периода времени;
2. кроме того, План аварийного восстановления Поставщика предусматривает следующее: (a) Поставщик уведомит Citi в письменной форме в течение двух (2) часов о любой аварии, которая может негативно сказаться на размещенных сервисах; (b) Поставщик предоставит Citi в течение 24 часов после такого уведомления план дальнейшего предоставления Размещенных сервисов на альтернативном объекте; (c) Размещенные сервисы должны быть полностью готовы к работе в течение 48 часов с момента первоначального уведомления;
3. Поставщик соглашается по запросу предоставлять информацию, необходимую Citi для разработки плана аварийного восстановления и плана обеспечения непрерывности деятельности, которые будут работать в соответствии с планом аварийного восстановления и планом обеспечения непрерывности бизнеса Поставщика; а также
4. если часть объектов Поставщика выйдет из строя, Поставщик будет обслуживать Citi на том же уровне, что и других коммерческих клиентов.

14.5 Изменения в плане аварийного восстановления

Поставщик может изменить свой План аварийного восстановления при условии, что эти изменения не ухудшат План аварийного восстановления таким образом, что они могут отрицательно повлиять на услуги (например, приведут к увеличению целевого времени восстановления). Поставщик должен незамедлительно сообщить Citi обо всех изменениях в своем Плане аварийного восстановления и, по запросу Citi, объяснить изменения таким образом, чтобы Citi полностью поняла эти изменения и смогла отреагировать на них.

14.6 План аварийного восстановления субподрядчиков

Поставщик гарантирует, что все Субподрядчики Поставщика имеют План аварийного восстановления и соответствующие средства контроля для обеспечения непрерывности коммерческой деятельности, которые соответствуют требованиям Citi в отношении поставщиков. Поставщик должен обеспечить надлежащий надзор за Субподрядчиками, в том числе он должен выполнять периодическую проверку таких средств контроля и результатов проверок, и обеспечить своевременное устранение любых выявленных недостатков.

14.7 Запуск плана аварийного восстановления и уведомление о кризисе

Поставщик незамедлительно уведомит основное деловое контактное лицо в Citi:

1. Когда Поставщик применяет свой План аварийного восстановления; а также
2. При возникновении любого кризиса, угрозы, предупреждения или киберсобытия в отношении Поставщика или его субподрядчиков, которые с достаточной вероятностью могут оказать неблагоприятное воздействие на услуги или продукты, предоставляемые Citi.

14.8 Тестирование

Все аварийные ресурсы и планы Поставщика должны быть испытаны в течение 120 дней после их внедрения в производственный процесс (90 дней в случае приложений, классифицированных Citi как Enterprise Critical). Такие испытания должны проходить не реже одного раза в год (каждые 12 месяцев). Тестирование должно показывать способность Поставщика обеспечивать во время восстановления уровень обслуживания по всем продуктам и услугам, предоставляемым Citi. Тестирование должно быть всеобъемлющим и включать в себя весь объем услуг, предоставляемых Citi. Поставщики обязаны уведомить Citi не менее чем за 30 календарных дней до тестирования восстановления по продуктам/услугам, предоставляемым Citi. Citi может участвовать в испытании Поставщиком восстановления приложений, используемых Citi для проверки функциональных возможностей приложения в среде восстановления, или наблюдать за этим процессом. Если Citi желает принять участие, Поставщик перед проведением тестирования предоставит Citi цели тестирования, план тестирования и процедуры подключения к тестовому сайту. В течение десяти (10) рабочих дней после завершения каждого теста Поставщик предоставит Citi сводку целей тестирования, план тестирования и результаты тестирования, включая сроки, необходимые для восстановления и доказательства результатов тестирования (например, скриншоты).

14.9 Подтверждение объема

Поставщик, размещающий у себя приложения, классифицированные Citi как Enterprise Critical, должен продемонстрировать, что объем производства может быть обеспечен в его среде COB или среде аварийного восстановления. Citi и Поставщик должны согласовать методологию, которая будет использоваться для такого подтверждения объема.

14.10 Использование систем Citi для предоставления услуг

По запросу Citi или Аффилированных лиц Citi Поставщики, использующие системы Citi, должны участвовать в проводимых Citi учениях по аварийному восстановлению.

14.11 Обработка результатов испытаний

Если какие-либо результаты проведенных Поставщиком испытаний покажут, что задачи испытания не были достигнуты или применимое целевое время восстановления (RTO) не было соблюдено, Поставщик должен провести анализ основных причин таких неудач и незамедлительно устранить все выявленные недостатки. После внесения таких исправлений Поставщик проводит повторный тест не позже, чем через сто двадцать (120) календарных дней (90 календарных дней, если Citi классифицирует приложения как Enterprise Critical) после предыдущего неудачного теста (или в сроки, указанные в соответствующем Рабочем наряде).

14.12 Регулирование кризисной ситуации

Помимо плана обеспечения непрерывности деятельности, у Поставщика должен быть план действий в кризисных ситуациях для управления операциями по восстановлению. План действий в кризисных ситуациях, составленный Поставщиком, должен содержать как минимум имена лиц, наделенных достаточными полномочиями для начала восстановительных мероприятий, устанавливать протоколы коммуникаций и доведения до вышестоящих инстанций для сбора и распространения информации о кризисной ситуации, а также включать протоколы уведомления и доведения до вышестоящих инстанций для взаимодействия с Citi в случае возникновения кризисной ситуации.

14.13 Оценка непрерывности деятельности

Поставщики обязаны пройти Процесс оценки непрерывности деятельности сторонних лиц Citi, целью которого является оценка соответствия политик, процедур и средств контроля Поставщика требованиям Citi, требованиям законодательства и/или нормативным актам (регулирующим деятельность Citi или Поставщика) в области непрерывности деятельности. Процедура оценки проводится в формате анкет, на которые Поставщик предоставляет ответы с документальными доказательствами, а также может включать в себя посещение объектов Поставщика. Если в ходе оценки будут выявлены проблемы или подозрения, Citi зафиксирует результаты проверки и вместе с Поставщиком разработает способ устранения этих проблем. Поставщики обязаны в кратчайшие сроки вносить необходимые поправки и/или внедрять необходимые компенсирующие средства контроля для удовлетворительного для Citi в разумных пределах решения проблем, выявленных компанией.

14.14 Устойчивость деятельности

Критически важные бизнес-услуги — это услуги, которые в случае перебоев с поставками могут оказать существенное отрицательное влияние на Citi, клиентов или финансовую систему. Поставщик должен обеспечить, чтобы любые сбои в доставке элементов услуг, которые либо представляют собой критически важные бизнес-услуги, либо поддерживают предоставление критически важных бизнес-услуг Citi, согласно предоставляемым Citi указаниям (далее — «Критически важные бизнес-услуги»), не выходили за рамки срока, установленного Citi, или иным образом не нарушали какие-либо соответствующие показатели, установленные Citi (далее — «Допустимое воздействие»), о чем Citi время от времени уведомляет Поставщика. Допустимое воздействие выражается в виде показателя с четко установленными сроками, который представляет собой время, в течение которого может быть нарушено предоставление услуг. Citi и Поставщик должны ежегодно пересматривать Допустимое воздействие в рамках текущего процесса управления контрактами. В тех случаях, когда Citi требуется установить несколько Допустимых воздействий для отдельной Критически важной бизнес-услуги из-за требований более чем одного Регулирующего органа, Citi может установить отдельные Допустимые воздействия для такой Критически важной бизнес-услуги. Поставщик должен:

1. Уведомить Citi, как только станет известно, что ему не удалось (или есть достаточная вероятность того, что не удастся) предоставить какую-либо услугу в рамках соответствующего Допустимого воздействия, установленного Citi, вместе с объяснением причин любых предполагаемых или фактических сбоев и мер, предпринимаемых для смягчения последствий такого сбоя.
2. По запросу оказывать Citi разумную помощь, позволяющую определить, какие люди, процессы, технологии, средства и информация необходимы Поставщику для предоставления услуг, обеспечивающих выполнение Критически важных бизнес-услуг.
3. Предоставлять обоснованную помощь Citi, чтобы позволить ей выполнять следующие действия:
 - a. любые внутренние сценарии тестирования способности Поставщика оставаться в пределах Допусков к воздействиям для каждой Критически важной бизнес-услуги в случае серьезного, но вероятного нарушения его деятельности или деятельности Поставщика; а также
 - b. использовать полученные результаты по итогам испытаний на основе сценария, чтобы Citi могла выявлять недостатки и действия, необходимые для повышения способности Поставщика эффективно реагировать на будущие сбои и восстанавливаться после них.

Если какое-либо внутреннее тестирование сценариев, проводимое Citi, выявит уязвимости или ограничения способности Поставщика предоставлять услуги в рамках соответствующих Допустимых воздействий, установленных Citi, а также ввиду неспособности Поставщика предоставить какие-либо услуги в рамках

соответствующих Допустимых воздействий, установленных Citi, стороны согласуют план (включая график реализации плана), гарантирующий, что Поставщик предпримет шаги, необходимые для устранения или смягчения таких уязвимостей или ограничений или устранения причины невозможности оставаться в пределах допустимого воздействия (если применимо), как только это станет практически возможным.

14.15 Организация эскроу

По запросу Citi Поставщики, (i) предоставляющие Citi лицензию на программное обеспечение для работы в среде Citi, или (ii) предоставляющие Citi размещенную услугу, должны сдать подлежащие сдаче на хранение материалы уполномоченному эскроу-агенту Citi и соблюдать график регистрации, действующий в отношении лица, сдающего такие материалы, или другие формы, необходимые эскроу-агенту в отношении материалов, подлежащих сдаче на хранение, в соответствии с применимым соглашением об эскроу. После этого в течение оставшейся части срока действия применимого соглашения в отношении лицензии или размещенной услуги Поставщик должен сдавать обновленные версии материалов, подлежащих сдаче на хранение, эскроу-агенту, чтобы гарантировать, что Исходный код и другие материалы, подлежащие сдаче на хранение, соответствуют последней версии программного обеспечения, применимой к версии программного обеспечения или размещенных услуг, используемых Citi. Обновления исходного кода и других материалов, подлежащих сдаче на хранение, должны быть переданы эскроу-агенту в течение тридцати (30) дней с даты обновления программного обеспечения, лицензия на которое была предоставлена Citi, или даты внесения изменений в размещенные услуги, используемые Citi. Поставщик должен полностью соблюдать все обязательства и требования в отношении лица, сдающего материалы, подлежащие сдаче на хранение, изложенные в соглашении об эскроу. Поставщик несет единоличную ответственность за все расходы и сборы в отношении эскроу, включая, помимо прочего, оплату установки этой услуги, годового взноса и взносов за размещение материалов, за предоставляемые услуги и любых других расходов и сборов, связанных с эскроу. В случае наступления события передачи материалов, подлежащих сдаче на хранение, эскроу-агент должен передать материалы, подлежащие сдаче на хранение, Citi или уполномоченному лицу Citi в соответствии с условиями базового соглашения и соглашения об эскроу.

Если исходный код (или другие материалы, подлежащие сдаче на хранение) предоставляется Citi или уполномоченному лицу Citi (прямо Поставщиком или эскроу-агентом в рамках выполнения ими своих обязательств по применимому соглашению об эскроу), исходный код и материалы, подлежащие сдаче на хранение, регулируются существующей лицензией согласно соответствующему соглашению между Поставщиком и Citi при условии, что каждая лицензия считается дающей Citi право на использование и изменение исходного кода и других материалов, подлежащих сдаче на хранение, что может быть обоснованно необходимо в следующих целях: (i) интегрировать программное обеспечение и другие материалы, подлежащие сдаче на хранение, в системы Citi и обеспечить их совместимость с системами Citi, (ii) обеспечить соответствие программного обеспечения и других материалов, подлежащих сдаче на хранение, Применимому

законодательству, отраслевым стандартам или рыночной практике, (iii) обеспечить, чтобы программное обеспечение или другие материалы, подлежащие сдаче на хранение, соответствовали актуальным технологическим достижениям; и (iv) обеспечить, чтобы программное обеспечение и другие материалы, подлежащие сдаче на хранение, выполняли коммерческие цели Citi и ее Аффилированных лиц в рамках существующей лицензии. Все версии программного обеспечения, содержащие изменения, разработанные Citi или от ее имени с использованием исходного кода, регулируются всеми положениями настоящего раздела и основного соглашения, и при этом Поставщик не имеет никаких прав, прав на владение и прав на участие в отношении таких изменений, а все права интеллектуальной собственности на любые изменения принадлежат исключительно Citi.

Поставщик примет коммерчески обоснованные меры во взаимодействии с третьими сторонами, предоставившими программное обеспечение, которое используется в Программном обеспечении, чтобы позволить Поставщику разместить исходный код такого стороннего программного обеспечения в материалах, подлежащих сдаче на хранение. В случае, если третья сторона отказывается предоставить Поставщику это право, Поставщик должен принять коммерчески обоснованные меры, чтобы применимое соглашение о лицензировании стороннего программного обеспечения было передано Citi после наступления события передачи материалов, подлежащих сдаче на хранение.

Исходный код, предоставляемый Citi в соответствии с настоящим разделом, регулируется существующей Лицензией на применимое лицензированное программное обеспечение или размещенные услуги при условии, что Citi может использовать и изменять исходный код и Программное обеспечение в связи со своими коммерческими и рабочими требованиями, чтобы Программное обеспечение содержало актуальные технологические достижения и соответствовало Применимому законодательству. Все версии программного обеспечения, содержащие изменения, разработанные Citi или от ее имени с использованием исходного кода, регулируются всеми положениями применимого соглашения, и при этом Поставщик не имеет никаких прав, прав на владение и прав на участие в отношении таких изменений, а все права интеллектуальной собственности на любые изменения принадлежат исключительно Citi.

15 МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ПРОВЕРКИ АНКЕТНЫХ ДАННЫХ

Применимо ко всем Сторонним поставщикам, предоставляющим услуги для компании Citi.

15.1 Обзор — проверка анкетных данных

Проверка анкетных данных должна проводиться в соответствии со всеми применимыми местными законами и нормативно-правовыми требованиями. Представители Поставщика, сотрудники Поставщика и Субподрядчики обязаны в установленной форме предоставить все описанные в настоящем документе

данные и сведения о себе. Фальсификация или отсутствие информации, представленной в резюме, в ходе собеседования, в форме регистрации или в ходе процесса адаптации, независимо от того, когда это будет выявлено, может являться основанием для отказа или прекращения работы в Citi в соответствии с местным законодательством. Неблагоприятные результаты любой проверки, независимо от того, когда это будет выявлено, могут также представлять собой основания для отказа или прекращения работы с Citi в соответствии с местным законодательством.

Дополнительную информацию о проверке анкетных данных можно найти на сайте https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 Сбор основной информации и проверка личности

Прежде чем сотрудник Поставщика начнет выполнять задание Citi, Поставщик должен собрать информацию об этом лице, такую как его имя и фамилия, почтовый адрес, адрес постоянного места жительства (если не совпадает с почтовым адресом), номер телефона и адрес электронной почты (при наличии). Персонал Поставщика также должен предоставить документы, удостоверяющие личность Персонала. В этом случае может потребоваться предоставить информацию и (или) документы, подтверждающие номер удостоверения личности государственного образца, идентификационную карту государственного образца с фотографией или паспорт.

15.3 Проверка в списках санкций

Весь персонал Поставщика, выполняющий работу от имени Citi, или лицо, владеющее 25 % (или более) Поставщика Citi, включая Субподрядчиков, независимо от наличия доступа к данным, системам, сетям Citi И (ИЛИ) помещениям Citi, должны быть проверены на присутствие в Списке граждан особых категорий и запрещенных лиц («SDN») Управления по контролю за иностранными активами («OFAC») Министерства финансов США, списке регионов и юрисдикций, на которые наложены санкции США («Санкции США»), а также в любом изданном списке, содержащем названия юрисдикций, на которые наложены санкции за пределами США, включая Сводный список финансовых санкций Европейского союза, Сводный список Совета безопасности ООН, Список санкций Великобритании и списки, соответствующие законам и нормативно-правовым требованиям, применимым к местной юрисдикции («Санкции за пределами США»). Списки OFAC выложены в открытом доступе на этом сайте: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Соблюдение миграционного законодательства

Поставщик обязан продемонстрировать, что он соблюдает и внедряет протоколы, позволяющие подтвердить, что весь его персонал имеет право работать в стране, в которой он получил назначение. Кроме того, Поставщик обязан: (1) обеспечить, чтобы весь его персонал имел разрешение на работу, и (2) соблюдать все

применимые законы, нормативно-правовые требования и политики (включая требования в отношении правомочности и подтверждения трудоустройства). Поставщик также должен продемонстрировать и обеспечить наличие протоколов, обеспечивающих соблюдение его персоналом всех применимых иммиграционных законов и нормативно-правовых требований, а также то, что его персонал имеет соответствующий статус или категорию визы для выполнения назначенных ему заданий и выполняемых им видов деятельности.

15.5 Данные о предыдущих местах работы

Поставщик должен проверить данные о предыдущих местах работы своих сотрудников за последние 7 (семь) или 10 лет, если такая проверка требуется согласно местным нормативно-правовым требованиям. История занятости физического лица подлежит проверке с целью убедиться, что сведения о работодателях, должностях, датах и обязанностях являются достоверными. Сотрудники поставщика также должны сообщить, работали ли они ранее на постоянной основе в Citi или ее компаниях-предшественниках и выполняли ли они ранее задания Citi или ее компаний-предшественников в качестве консультанта или временного работника (к таким компаниям-предшественникам относятся, помимо прочего, Citibank, Citicorp, Travelers, Salomon Brothers и/или Smith Barney).

15.6 Сведения о полученном образовании

Поставщики должны проверять уровень образования своих сотрудников. К информации, подлежащей проверке, относится информация о периоде обучения, название учебного заведения, его адрес и полученные степени.

15.7 Данные о судимости

В разрешенных законом случаях, сотрудники и субподрядчики Поставщика обязаны уведомить Citi в случае наложения ареста, вызова в суд, получения судебной повестки, предъявления обвинения в суде, привлечения к уголовной ответственности или признания виновным в уголовном преступлении, в том числе в случае признания своей вины или неопротестованного обвинения, а также участия в досудебном разрешении уголовно-правового спора или вступления в аналогичные договоренности. В разрешенных законом случаях административная проверка данных о судимостях и (или) проверка отпечатков пальцев должны быть завершены до начала первого рабочего дня сотрудника. Совершение уголовных преступлений, связанных с хищением, мошенничеством, недобросовестностью, злоупотреблением доверием, а также подобных преступлений, имеющих другое определение согласно местному законодательству, за исключением случаев, когда это запрещено законом, может привести к отказу и/или признанию несоответствия предлагаемой должности в Citi. Приговоры по другим нарушениям могут привести к отказу и/или признанию несоответствия предлагаемой должности, исходя из применимых местных законов и нормативных актов.

15.8 Повторные проверки

В случае повторного назначения сотрудника на должность, связанную с Citi, персонал Поставщика обязан пройти повторную проверку. Дополнительную

информацию о требованиях к повторной проверке можно получить по адресу https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Международные переводы

Все проверки должны проводиться в соответствии с нормативными требованиями страны, в которой сотрудник назначен на должность. Если сотрудник Поставщика переведен в другую страну, он обязан пройти повторную проверку согласно требованиям соответствующей страны.

16 РАСХОДЫ

Поставщики, которые по договору вправе требовать возмещения деловых расходов

16.1 Общая информация

Citi должна возмещать только обоснованные расходы, связанные с коммерческой деятельностью, которые были заранее утверждены Citi в письменной форме, и которые были понесены Поставщиком в связи с предоставлением продуктов и услуг Citi, соответствуют положениям действующего Договора, политики Operating Expense Governance Citi и соответствующим данной Политике стандартам и процедурам, в зависимости от ситуации, а также надлежащим образом подтверждены квитанциями, счетами, транспортными документами и другими документами, которые Citi считает приемлемыми.

16.2 Возмещение расходов

Расходы должны быть надлежащим образом задокументированы и указаны в счете, выставляемом в адрес Citi в соответствии с требованиями Citi к выставлению счетов. Сотрудник Citi не должен нести расходы Поставщика от имени Поставщика. Документы, подтверждающие расходы, представляемые Citi с целью возмещения по обоснованным и утвержденным статьям расходов, должны включать в себя (помимо всех других требований к выставлению счетов):

1. бизнес-цель расходов;
2. сумма и описание расходов;
3. место и дата понесения расходов;
4. название и описание проекта, для которого Поставщик предоставляет услуги;
5. имена представителей Citi, запрашивающих услуги, по которым были совершены расходы, и характер их связи с компанией; а также
6. номер заказа на закупку (если применимо).

Для получения информации о разрешенных коммерческих расходах, подлежащих возмещению, свяжитесь с основным контактным лицом Citi. Подтверждающие квитанции, счета, транспортные документы и другие документы, которые Citi считает приемлемыми, следует предоставлять вместе с требованием о возмещении. Запросы на возмещение расходов должны, при необходимости,

соответствовать положениям применимого Контракта или Политики управления расходами Citi, а также соответствующим Стандартам и Процедурам, и утверждаться соответствующим бизнес-спонсором и/или основным контактным лицом Citi, а также утверждаться лицом, должным образом уполномоченным и обладающим достаточной суммой для данного товара. Если заявка на возмещение не соответствует требованиям, расходы не подлежат возмещению.

17 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ)

Применимо к Поставщикам, включая Субподрядчиков, которые получают доступ к любой информации Citi, классифицированной и определенной в Приложении, обрабатывают, хранят или управляют ею; или осуществляют хостинг Интернет-приложений под брендом Citi; или имеют возможность подключения к сетевым ресурсам Citi; и/или которым требуется доступ к помещениям Citi без сопровождения.

17.1 Общая информация

Этот раздел содержит минимальные требования к Поставщикам Citi, включая субобработчиков или субподрядчиков Поставщиков, которые хранят, обрабатывают, управляют или получают доступ к информации Citi или осуществляют хостинг приложений Citi или имеют подключение к сети Citi, в отношении необходимых мер защиты информации, которых требует Citi. Эти требования обеспечивают защиту информации в соответствии с применимыми законодательными и регуляторными требованиями и самыми высокими отраслевыми стандартами (например, ISO / IEC 27001/2) в местах, где Citi и ее Поставщики осуществляют свою деятельность. Если местным законодательством, нормативными актами или соответствующими отраслевыми стандартами предусмотрены более строгие, по сравнению с настоящими Требованиями, стандарты, Поставщики обязаны соблюдать требования местного законодательства, нормативных актов или отраслевых стандартов. Кроме того, другие политики Citi и договорные условия и положения могут потребовать от Поставщика соблюдения дополнительных методов и процедур обеспечения информационной безопасности. В случае внедрения дополнительных методов или процедур обеспечения информационной безопасности Поставщик обязан убедиться, что эти методы и процедуры не вступают в противоречие с минимальными требованиями настоящего раздела.

17.2 Политика информационной безопасности и управление информационной безопасностью

Политику и стандарты информационной безопасности Поставщик должен зафиксировать в документах. Управление политикой должно включать в себя четко определенные роли и обязанности, а также ежегодный обзор/обновление политики и стандартов для обеспечения соответствия актуальному состоянию технологий, отраслевым стандартам, правовым и регуляторным требованиям.

17.3 Разделение обязанностей

Поставщик обязан внедрить процессы, не позволяющие ни одному физическому лицу одновременно выполнять две коммерческие операции или ИТ-операции или две операции с Системой, содержащей конфиденциальную информацию, имея постоянный доступ к одному и тому же действию, изменению, информационной системе или операции, без разрешения или оповещения, за исключением случаев, когда для снижения рисков предусмотрены достаточные средства исправления ситуации.

Таблица А

Функции	Описание функции
Разработка и проектирование	Проектирование, создание или изменение программного обеспечения, оборудования и параметров. Примеры: - Разработка и создание нового кода приложения и соответствующих схем баз данных. - Проектирование продуктов инфраструктуры и прикладных компонентов. - Настройка технологических продуктов с целью их интеграции с программным обеспечением и услугами.
Утверждение	Утверждение поддержки подлежащих внедрению изменений кода.
Внедрение и администрирование систем	Установка, развертывание и администрирование программного обеспечения, оборудования и изменений параметров. Примеры: - Выполнение автоматического или ручного выпуска кода в производственную инфраструктуру. - Установка технологического продукта или прибора. - Запуск или остановка служб для поддержки устранения неполадок и проблем для систем с производственными данными.
Проверка активности по привилегированным идентификаторам	Проверка действий по управлению изменениями или событиями, связанных с системой безопасности (например, журналы регистрации событий).
Администрирование идентификаторов	Добавление, изменение и удаление идентификаторов (пользователей, FID и ботов), прав и паролей.

Функции в рамках бизнес-структуры	Описание функции
Инициирование сделок бизнес-структуры	Инициирование (которое также называется вводом, организацией или созданием) сделок бизнес-структуры и изменение информации о клиентах.
Утверждение сделок бизнес-структуры	Утверждение (которое также называется авторизацией, проверкой или выпуском) сделок бизнес-структуры.
Функция IT	Описание функции
Сетевые операции	Управление устройствами и операционная поддержка продуктов, которые предоставляют услуги сетевой инфраструктуры. Примеры: сетевые маршрутизаторы, переключатели, брандмауэры и службы доменных имен.
Операции, не относящиеся к сети	Управление устройствами и операционная поддержка продуктов, которые не предоставляют услуги сетевой инфраструктуры. Примеры: серверы, телефоны и компьютеры.

17.4 Обязанности руководства в сфере информационной безопасности

Поставщики, размещающие у себя интернет-приложения с фирменным оформлением Citi и (или) получающие доступ к информации Citi, классифицированной как Конфиденциальная или более ценная, обязаны пройти Процесс оценки уровня информационной безопасности третьих сторон Citi (TPISA), целью которого является оценка соответствия политик, процедур и средств контроля Поставщика требованиям Citi, требованиям законодательства и/или нормативным актам (регулирующим деятельность Citi или Поставщика) в области информационной безопасности.

Такая оценка подразумевает анкетирование, в ходе которого Поставщик предоставляет обоснованные ответы на вопросы об уровне безопасности, и посещение объектов, используемых Поставщиком для хранения, обработки, управления Конфиденциальной информацией или информацией более высокого уровня защиты Citi или предоставления доступа к ней третьей стороне. Кроме того, отдел TPISA Third Party Continuous Monitoring Team может осуществлять контроль над Поставщиком с помощью инструментов контроля за кибербезопасностью, которые используют общедоступную информацию для выявления уязвимых систем, хост-узлов, приложений и серверов с выходом в Интернет в отношении таких проблем, как наличие программного обеспечения с истекшим сроком эксплуатации, эксплуатируемых открытых портов, уязвимостей и других нарушений. Если в ходе TPISA будут выявлены недостатки безопасности, Citi зафиксирует результаты проверки и направит уведомление Поставщику, чтобы впоследствии вместе разработать способ устранения этих недостатков.

Поставщики обязаны в кратчайшие сроки внести необходимые исправления и (или) внедрить необходимые альтернативные средства контроля для решения проблем Citi по усмотрению Citi. На это отводится не более 180 календарных дней для проблем высокого риска, 240 календарных дней для проблем среднего риска и срок до следующей даты проверки соблюдения нормативно-правовых требований для проблем низкого риска в соответствии с оценкой риска, проведенной Citi.

1. Поставщик должен регулярно проводить оценку своей деятельности и соответствующих средств контроля согласно его собственным стандартам, политикам и процедурам информационной безопасности. Периодические оценки должны включать в себя, как минимум, следующее:
 - a) оценку процессов, которые Поставщик использует для обеспечения соответствия собственной политике и собственным стандартам информационной безопасности;
 - b) оценку вспомогательных ресурсов (например, приложений и инфраструктуры, используемых Поставщиком) и процессов информационной безопасности, используемых субподрядчиками Поставщика (при наличии) для поддержки их операционной деятельности или предоставления Citi должна возможности осуществлять такую оценку. Необходимо обеспечить соответствие требованиям в случае подписания третьим лицом нового или продления существующего договора с субподрядчиком, который осуществляет доступ к информации Citi, расцениваемой Citi как Конфиденциальная или имеющей более высокий уровень защиты, обработку такой информации, управление такой информацией или ее уничтожение.
2. Выявленные в результате Оценки рисков информационной безопасности (например, TPISA) проблемы необходимо фиксировать и отслеживать до момента устранения с предоставлением Citi доказательств устранения.
3. Если подразделение управления информационной безопасности Поставщика переезжает в другую страну, Поставщик обязан получить письменное разрешение Citi до осуществления данного переезда.
4. Если Поставщик приобретает новую компанию, он обязан провести оценку приобретаемой компании на предмет соответствия настоящим Стандартам.
5. Поставщик не вправе передавать на аутсорсинг функции управления безопасностью, включая, помимо прочего, управление брандмауэром, управление конфигурацией безопасности, управление внесением исправлений или администрирование информационной безопасности (ISA), если они относятся к системам, используемым для хранения, обработки и (или) передачи информации Citi, за исключением случаев, когда это предварительно одобрено Citi в письменной форме.
6. Если Поставщик размещает у себя программное обеспечение или веб-сайт, содержащий информацию Citi или фирменное оформление Citi, он должен регулярно проводить оценку уязвимости, в соответствии со Стандартом тестирования системной безопасности (SSTS) Citi и своевременно, в сроки, предусмотренные таким Стандартом, устранять обнаруженные во время оценки проблемы. Поскольку SSTS не утвержден для внешнего распространения, Поставщики должны вместе со своим менеджером по работе с Citi обеспечить соответствие справочной документации. Кроме

того, Поставщик должен соблюдать соответствующие стандарты обеспечения информационной безопасности ISO/IEC 27001 (или последующие стандарты обеспечения информационной безопасности, устанавливающие более строгие стандарты и протоколы) и соблюдать положения, касающиеся информационной безопасности, содержащиеся в настоящем Разделе (17).

7. Если Поставщику требуется доступ к серверам и/или информационным системам во внутренней сети Citi, он должен уведомить об этом свое основное контактное лицо в Citi с целью соблюдения актуального процесса обеспечения подключения к сети.
8. Поставщик должен незамедлительно уведомить соответствующее контактное лицо Citi (Ответственного за деловую активность (BAO)) о любом несанкционированном доступе, приобретении, потере, повреждении или удалении информации Citi или о любом другом нарушении функционирования системы безопасности информационных систем, используемых для хранения, обработки или передачи информации Citi.
9. Поставщик должен убедиться, что при всех действиях высокого риска или при внесении изменений в конфиденциальную информацию используются журналы регистрации событий, в которых такие действия должны быть назначены конкретным лицам, совершивших их.
10. Поставщик обязан обеспечить маскировку конфиденциальной информации или информации более высокого уровня защиты на экране и на бумаге (в том числе, например, отчеты о мониторинге, исключениях и регуляторной базе и другие отчеты).
11. Поставщик обязан наложить ограничения на печать, запись и копирование конфиденциальной информации, в том числе на своих собственных устройствах. Поставщик обязан вернуть или уничтожить всю информацию Citi в оговоренный момент времени в ходе выполнения соглашения или в конце соглашения, если иное не запрещено законом или нормативно-правовыми требованиями.
12. Поставщик обязан проследить за тем, чтобы весь персонал поставщика (сотрудники, подрядчики, временные сотрудники, субподрядчики), имеющие доступ к информации Citi, подписали соглашение о неразглашении информации или сохранении конфиденциального характера информации.
13. Сотрудники Поставщика должны получить руководство для сотрудников или аналогичный документ с описанием дисциплинарной процедуры, которая применяется в случае несоблюдения и нарушений кодекса поведения Поставщика и кадровых политик; предоставление данных документов должно быть частью процесса адаптации сотрудников.
14. Поставщик разрабатывает процедуру для возвращения себе всех активов при прекращении трудового договора или увольнении сотрудника или лица, не являющегося сотрудником.
15. Если какая-либо Конфиденциальная информация имеется в наличии или каким-либо образом хранится на веб-сайте или в системе, доступной через Интернет, Поставщик должен раскрыть данную информацию Citi. Такое разглашение может быть включено в описание Услуг. Если Поставщик имеет или хранит Конфиденциальную информацию Citi, Поставщик требует проведения аудита SSAE 18 (или любой принятой вместо него авторитетной

оценки, утвержденной Citi) один раз в год в течение срока действия настоящего Соглашения и предоставляет Citi не реже одного раза в год копию отчетов о результатах такого аудита SSAE 18 или любой принятой вместо него авторитетной оценки, утвержденной Citi.

16. Если Поставщика приобрело другое юридическое лицо или Поставщик приобретает другое юридическое лицо в результате слияния или приобретения или аналогичной сделки, и такая транзакция имеет шанс повлиять на Услуги, Поставщик должен незамедлительно уведомить об этом Citi в письменной форме, а также провести оценку информационной безопасности полученного юридического лица в соответствии с настоящими Требованиями, чтобы гарантировать, что такое приобретение или слияние не повлияет на соблюдение данных Требований.

17.5 Риск информационной безопасности, связанный с субподрядчиками

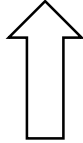
Поставщик обязан требовать, чтобы все субподрядчики, имеющие доступ к конфиденциальным данным Citi или данным Citi более высокого уровня защиты, проходили обязательную проверку информационной безопасности перед заключением и, периодически, после заключения договора субподряда; проверки проводят квалифицированные специалисты в области Информационной безопасности (ИБ). Такую оценку следует проводить в соответствии с утвержденным руководством процессом, который охватывает все этапы процесса оценки от начала до решения проблем. Оценка ИБ субподрядчика должна включать в себя анкету или эквивалентный инструмент, который оценивает позицию субподрядчика в сферах ИБ в соответствии со сферами, включенными в Анкету оценки ИБ третьих сторон (TPAQ) Citi, и она должна включать в себя логический метод расчета риска ИБ, связанного с привлечением субподрядчика. Поставщик должен отслеживать выполнение оценки и управлять выявленными проблемами и планами корректирующих действий до их завершения.

17.6 Ответственность за активы

1. Поставщик обязан вести учет всех приложений и оборудования, находящихся под его контролем и используемых для хранения, обработки и/или передачи информации Citi.
2. Поставщик должен обеспечить ведение учета информационных активов Citi под его контролем в соответствии с процедурой, применяемой для надлежащего поддержания точности и полноты таких записей.
3. Поставщик несет ответственность за защиту всей информации Citi под его контролем.
4. Поставщик обязан проследить за тем, чтобы пользователи ответственно соблюдали отраслевые практики работы с информацией.
5. Доступ пользователей к персональным внешним хранилищам электронной почты в Интернете и облачным хранилищам должен быть отделен от глобальной сети Поставщика, в которой хранится информация Citi.

17.7 Классификация и обработка информации

Citi классифицирует информацию согласно приведенной ниже таблице «Классификация информации». Определения и примеры каждой из перечисленных ниже классификаций можно найти в Приложении.

ИНФОРМАЦИЯ С ОГРАНИЧЕННЫМ ДОСТУПОМ	Наиболее секретная
СЕКРЕТНАЯ ИНФОРМАЦИЯ, КОТОРАЯ ПОЗВОЛЯЕТ УСТАНОВИТЬ ЛИЧНОСТЬ (PII)	
КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ, КОТОРАЯ ПОЗВОЛЯЕТ УСТАНОВИТЬ ЛИЧНОСТЬ (PII)	
КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ	
ВНУТРЕННЯЯ ИНФОРМАЦИЯ, КОТОРАЯ ПОЗВОЛЯЕТ УСТАНОВИТЬ ЛИЧНОСТЬ (PII)	
ВНУТРЕННЯЯ ИНФОРМАЦИЯ	
ОБЩЕДОСТУПНАЯ ИНФОРМАЦИЯ	Наименее секретная

1. Опираясь на классификацию информации Citi, Citi должна совместно с Поставщиком определить уровень безопасности, который необходим для защиты информации, а Поставщик обязан обеспечить установление достаточных средств контроля, наряду с уровнями повышенной или усовершенствованной защиты, которые впоследствии может задать Citi.
2. Служебная информация или информация более высокого уровня защиты должна храниться на управляемых третьими сторонами устройствах, являющихся предметом договора между третьей стороной и Citi, содержащего положения о конфиденциальности, не противоречащие политикам и стандартам Citi.
3. Если Поставщик допускает использование устройств, не принадлежащих компании, для хранения данных Citi (т.е. устройств, управляемых четвертой стороной), Поставщик обязан предусмотреть политику, которая подлежит специальному утверждению со стороны руководства и содержит установленные инструкции и процедуры мониторинга в отношении использования и уничтожения информации Citi.
4. Поставщик обязан всегда защищать информацию Citi от несанкционированного доступа, изменения или удаления.
5. Информация Citi, классифицируемая как конфиденциальная или информация более высокого уровня защиты и передаваемая через электронные портативные устройства (ETM), должна быть зашифрована с использованием утвержденного криптографического алгоритма, а получение такой информации необходимо подтверждать. Поставщик должен подтвердить, что ETM было получено предполагаемым адресатом.

Если подтверждение получения не получено к ожидаемой дате доставки, Поставщик должен уведомить об этом Citi.

17.8 Безопасная конфигурация

1. Поставщик должен использовать задокументированный стандарт обеспечения безопасной конфигурации для всех активов, позволяющих хранить, обрабатывать, передавать информацию Citi, или получать доступ к ней.
2. Поставщик обязан внедрить средства контроля за информационной безопасностью в свои процессы и процедуры выбора, разработки и развертывания приложений, продуктов и услуг.
3. Поставщик должен внедрить встроенную процедуру обеспечения безопасности во все системы, в которых хранится, обрабатывается и/или посредством которых осуществляется передача информации Citi.
4. У Поставщика должны иметься безопасные образы, или шаблоны для всех систем.
5. Все заданные по умолчанию учетные записи и пароли пользователей в поддерживаемых поставщиком системах, сетевых устройствах и приложениях подлежат обязательному удалению и/или изменению.
6. Любая скомпрометированная система или услуга должна быть перестроена и настроена с использованием образа или шаблона, имеющего доказанную целостность.
7. Любые изменения, вносимые в безопасную конфигурацию, должны быть утверждены руководством с использованием принятой Поставщиком процедуры управления изменениями.
8. Поставщик должен уведомить Citi о любых изменениях в безопасной конфигурации.
9. Процедура безопасной конфигурации должна включать в себя инструменты для автоматической проверки конфигурации безопасной / стандартной сборки в ходе развертывания системы в среде ее эксплуатации, а также постоянный мониторинг в целях обеспечения соблюдения и отслеживания отклонений от базовой конфигурации.

17.9 Требования в отношении шифрования

Поставщику запрещается передавать конфиденциальную информацию или информацию с более высокой классификацией без шифрования. Информация, классифицируемая как конфиденциальная или более секретная, должна быть подвергнута **сквозному** шифрованию с помощью использованием утвержденных Citi инструментов или решений. Утвержденные протоколы и соответствующие номера версий при шифрованной передаче данных:

1. При передаче информации о проверке подлинности и авторизации: SAML v2.0, OAuth v2.0 (только авторизация).
2. Для защиты каналов связи и связанного с ними обмена ключами разрешается использовать только следующие Протоколы сетевой безопасности:
 - а) Предпочтительно использование TLS v1.3. Допускаются все пакеты TLS v1.3. Если TLS v1.3 является единственным разрешенным протоколом, дополнительная проверка не

- требуется.
- b) Если TLS v1.3 не поддерживается на техническом уровне, а используется TLS 1.2, тогда класс B (или более высокий) от SSL Labs является приемлемым в данный момент, и дополнительная проверка не требуется.

Данные, постоянно хранящиеся в среде Третьего лица Citi или передаваемые при обмене, должны быть полностью зашифрованы с использованием одобренных Citi инструментов или решений. Одобренные алгоритмы и длины ключей для шифрования данных:

1. **Расширенный стандарт шифрования (AES):** утвержденные длины ключей: 256 или более бит. Ограниченные режимы: режим электронной кодовой книги (ECB) запрещен, за исключением случаев, когда объем открытого текста меньше или равен длине блока. Шифрование диска: требуется использовать AES с 256-битным ключом. AES со 128-битовым ключом разрешен в качестве шифра TLS. Как ожидается, он будет заменен на 256-битовый (или с большим количеством битов) до 31 декабря 2028 года, чтобы Citi соблюдала международные сроки (Ref, NIST 8547 IPD).
2. **ChaCha20 (поточковый шифр для соответствующих вариантов использования):** утвержденные длины ключей: 128 или 256 битов, с 96-битовым одноразовым случайным числом и 32-битовым отсчетом блоков или 64-битовым одноразовым случайным числом и 64-битовым отсчетом блоков. Максимальный размер данных: 16 петабайтов.

Утвержденные криптосистемы с открытым ключом, обмен ключами, механизмы согласования, профиль сообщения и функции формирования ключей:

Уведомление, связанное с квантовой готовностью поставщика. Поставщики должны представить свой план по охвату *таблицы 2* и *таблицы 4* NIST IR 8547 (ipd) отделу Citi Quantum Readyence Program через ([ссылка на опрос](#)).

1. **Криптосистемы с открытым ключом и минимальные размеры ключа:**
 - a) Rivest–Shamir–Adleman (RSA): 2048 бит.
 - b) Алгоритм цифровой подписи (DSA): 2048 бит. DSA нельзя использовать для защиты данных Citi, обрабатываемых или хранящихся вне Citi.
 - c) Алгоритм цифровой подписи на основе эллиптических кривых (ECDSA): 256 бит и как указано в ANSI X9.62 с рекомендованными кривыми NIST.
2. **Механизмы обмена ключами и соглашения, а также минимальные размеры ключей:**
 - a) Алгоритм Диффи-Хеллмана (DH) / Эфемерный алгоритм Диффи-Хеллмана (DHE): 2048 бит.
 - b) Алгоритм Диффи-Хеллмана с использованием эллиптических кривых (ECDH) / Эфемерный алгоритм Диффи-Хеллмана с

использованием эллиптических кривых (ECDHE): 256 бит и как указано в ANSI X9.63 с рекомендованными кривыми NIST¹.

3. **Функции дайджеста сообщений:** создание ключа шифрования, длина которого превышает количество случайных битов в материале, используемом для генерации хэша, запрещено.
 - а) SHA-1 Приемлемо только для приложений без цифровой подписи. Семейство SHA-2, семейство SHA-3 и POLY-1305: приемлемо для всех приложений криптографических хэш-функций.
4. **Функции формирования ключей на основе пароля и минимальные требования.**
 - а) PBKDF2: с числом итераций не менее 10000 и как минимум с 16-байтовым случайным числом, присоединяемым к паролю.
 - б) HKDF: необходимо дополнение и включение входного значения информации.
 - в) SCRYPT: минимальное количество раундов/коэффициент стоимости 10.
 - г) Использование NIST SP800-108 KDF для потокового шифрования запрещено. Приемлемыми являются режимы NIST SP 800-108 KDF, а именно Counter, Feedback and Double-Pipeline Iteration.
 - е) Рекомендуется Argon2.
5. **Хэш-функции паролей и минимальные требования:**
 - а) Bcrypt (для локального хранения аутентификационного материала): минимальное количество раундов/коэффициент стоимости не менее 10.
 - б) Рекомендуется использовать Argon2 или PBKDF2 для хэширования паролей при хранении паролей локально на любых системах или в любых средах, развернутых продуктами Поставщика.

17.10 Внешняя электронная почта

Требования к шифрованию личных электронных писем, содержащих конфиденциальную информацию Citi или информацию более высокого уровня защиты, которыми обмениваются Citi и Поставщик, когда нормативные акты и/или политика Поставщика запрещают Поставщику использовать одобренное Citi программное обеспечение или средства для межбонентского шифрования, могут быть в полной мере выполнены посредством шифрования при транспортировке (шифрование шлюз-шлюз по протоколу TLS). Утвержденные безопасные протоколы электронной почты:

1. **Шифрование на основе идентификации (IBE)** обеспечивает шифрование электронной почты и может использоваться только в клиентоориентированных решениях Citi, а также в защищенных системах электронной почты и электронной доставки.
2. **Протокол Mandatory TLS (MTLS)** обеспечивает шифрование сеанса (не шифрует полезные данные электронной почты) и может быть использован при взаимодействии с поставщиками, партнерами и

¹ Предпочтительно использование ECDHE.

клиентами, при наличии предварительной договоренности о его использовании.

3. **Почта с идентификацией ключей домена (DKIM)** обеспечивает аутентификацию источника и управление ключами и может быть использована поставщиками, партнерами и клиентами.

17.11 Частные сети

На частные сети, которые самостоятельно контролирует авторитетный полномочный орган и которые соответствуют отраслевым стандартам для осуществления финансовых операций между лицензированными или аккредитованными сторонами (например, SWIFT или центральным банком), требование к шифрованию конфиденциальной информации PII при передаче может не распространяться до тех пор, пока эти сети не обретут необходимую инфраструктуру для полноценного выполнения шифрования при передаче данных.

17.12 Голосовая связь и факс

При отправке конфиденциальной информации Citi или информации более высокого уровня защиты по факсу или обсуждении ее по каналу голосовой связи (включая IP-телефонию или VOIP) шифрование необязательно. При необходимости Поставщик должен разработать процедуры и инструкции по защите конфиденциальной информации или информации более высокого уровня защиты, передаваемой по этим каналам.

17.13 Управление криптографическими ключами и сертификатами

Термин «безопасная граница», используемый в данном разделе, относится к программе проверки криптографического модуля (CMVP), такой как Федеральный стандарт защиты информации (FIPS), проверяемой границей (FIPS 140-2/3 Уровень 2 является минимальным допустимым уровнем безопасности). (Конфиденциальные анклавы, например, AWS Nitro Enclaves, являются приемлемыми. Другие уникальные случаи границ между системами с разными уровнями безопасности должны быть утверждены Citi.)

1. Поставщик должен использовать текущие криптографические алгоритмы, соответствующие отраслевым стандартам, и минимальную длину ключа для шифрования и подписи (в том числе ключи SSH). Поставщик должен обеспечить гарантию через свой Процесс управления изменениями, когда такие алгоритмы и длины ключей обновляются для приведения в соответствие с отраслевыми стандартами.
2. Поставщик должен иметь официально задокументированный процесс управления жизненным циклом ключей, секретов и сертификатов с установленными средствами контроля для защиты чувствительных материалов от несанкционированного использования или раскрытия. Все события, связанные с жизненным циклом криптографических секретов и ключей, должны происходить только в пределах безопасной границы. Необходимо документировать весь доступ к привилегированным и безопасным границам. Поставщик должен предоставить диаграмму последовательности для всех ключевых

событий жизненного цикла, с указанием участников, организаций и границ.

3. Криптографические ключи должны иметь уникальное назначение и никогда не должны использоваться для какой-либо другой цели, например, запрещается использование одного и того же ключа шифрования для шифрования диска и шифрования данных или использование одного и того же ключа шифрования для шифрования полезной нагрузки и шифрования базы данных. Повторное использование криптографических ключей для нескольких арендаторов поставщиком SaaS запрещено по умолчанию и может быть разрешено только в ситуациях, не представляющих критически важное значение и имеющих низкий риск, которые связаны с информацией Citi, имеющей классификацию ниже, чем «Конфиденциальная информация, которая позволяет установить личность», «Секретная информация, которая позволяет установить личность» и «Информация с ограниченным доступом», при условии явного утверждения такого использования Советом архитектуры безопасности.
4. Для всех криптографических ключей (симметричных или асимметричных) закрытый ключ или материал закрытого ключа (например, сиды или часть закрытого ключа) ни при каких обстоятельствах не должны отображаться в виде открытого текста. Закрытый ключ или материал закрытого ключа (например, сид или часть закрытого ключа) никогда не должны покидать безопасную границу за исключением эфемерных ключей, таких как динамические сессионные ключи. Если проект требует передачи симметричного ключа, закрытого ключа или материала закрытого ключа между безопасными анклавами/границами привилегированного доступа, то он должен передаваться в только зашифрованном виде с использованием ключа Symmetric Key Wrapping Key или Public Key Transport Key только через взаимные туннели с шифрованием TLS; при этом такая передача должна быть утверждена Citi в письменной форме. В этих случаях ключ Private Key Transport Key никогда не должен пересекать безопасную границу привилегированного доступа, где он был создан.
5. Ключ Symmetric Key Wrapping Key должен быть разделен на два или более ключевых компонента и подвергнут XOR перед распространением и для ручного ввода/загрузки ключа. Ключ Symmetric Key Wrapping Key должен иметь соответствующие списки контроля доступа (ACL), связанные внутри безопасной границы, такие как валидированные модули CMVP. Кроме того, ключ Symmetric Key Wrapping Key не должен храниться за пределами безопасной границы.
6. Доступ людей, служб или автоматизированных агентов к хранилищам ключей или безопасным границам, содержащим закрытые ключи, секреты или материалы закрытого ключа (например, сиды или часть закрытого ключа), должен быть надлежащим образом разграничен с помощью средств контроля, предоставляющим доступ только уполномоченным сотрудникам или системам.
7. Каждый запрос на доступ к хранилищам ключей, содержащим закрытые или симметричные ключи, должен быть зарегистрирован и

задокументирован с указанием сведений о том, кто, когда и с какой целью получил доступ, для целей аудита.

8. Поставщик не должен использовать самостоятельно подписанные сертификаты, сертификаты с подстановочными знаками или сертификаты SSL по умолчанию.
9. Все криптографические ключи должны иметь определенные периоды действия, согласно рекомендациям, изложенным в NIST SP800-57, часть 1, версия 6. Обновление или ротацию ключей следует произвести до истечения срока их действия с учетом периодов изменений, планирования конфликтов и зависаний системы.
 - а) При замене истекшего сертификата повторное использование старой асимметричной пары ключей запрещено.
10. Криптографические ключи должны считаться скомпрометированными сразу же, как только возникает подозрение в компрометации целостности ключа, среды, в которой ключ хранится или передается, или конфиденциальности симметричного или закрытого ключа. Все скомпрометированные ключи должны быть удалены из эксплуатации, а все соответствующие сертификаты должны быть отозваны.
11. Беспроводные сети должны быть зашифрованы с помощью стандартных алгоритмов шифрования.
12. Поставщики, использующие любую форму криптографического механизма, должны применять стандартные для отрасли средства и методы управления ключами. Лицо, управляющее ключами, не должно выполнять функции руководителя по операционным вопросам.
13. Поставщики могут использовать облачные службы KMS и PKI только в том случае, если обеспечена совместимость с предоставляемыми через службы Citi Data Security Service службами PKI и KMS, а криптографический контроль не делегирован за пределы криптографического управления Citi.

17.14 Ответственность за управление доступом

Для защиты всех Систем, содержащих конфиденциальную информацию и используемых для хранения, доступа, управления, обработки или передачи Конфиденциальной информации Citi или информации более высокого уровня защиты от несанкционированного доступа, поставщик несет ответственность за соблюдение принципа наименьшей привилегии путем ограничения полномочий пользователей минимальным уровнем доступа, требуемым для каждой функции, и за управление обеспечением логического доступа ко всем системам и приложениям. Средства контроля должны быть полностью задокументированы и проверены. Предоставление и удаление доступа, включая сброс и активацию пароля, должны осуществляться посредством автоматического процесса, когда это возможно, для снижения рисков, связанных с возможными ошибками, вызванными человеческим фактором, и для соответствия отраслевым стандартам.

1. Поставщик несет ответственность за назначение прав доступа для всех пользователей в своей организации.

2. Поставщик обязан внедрить средства контроля доступа, обеспечивающие предоставление пользователям только тех прав и привилегий, которые строго необходимы им для выполнения своих должностных обязанностей.
3. Поставщик обязан внедрить процесс, гарантирующий, что все возможности доступа по умолчанию будут удалены, отключены или защищены, чтобы предотвратить несанкционированное использование систем.

17.15 Управление доступом пользователей

Поставщик должен обеспечить управление предоставлением логического доступа к системам и приложениям, осуществляющим обработку, хранение и/или передачу Конфиденциальной информации Citi или информации более высокого уровня защиты. Сюда входит следующее:

1. Идентификация и инвентаризация утвержденных систем аутентификации.
2. Требование, согласно которому для любого доступа к данным Citi требуется разрешение менеджера, или назначенного им сотрудника, и владельца системы. Поставщик несет ответственность за обеспечение того, чтобы любой из его сотрудников, имеющих доступ к данным Citi, имел доступ к таким данным по принципу необходимой информации.
3. Требование о том, чтобы любое сочетание привилегий/функций для конкретного пользователя не предусматривалось, если оно представляет собой конфликт интересов или нарушение правил maker-checker.
4. Процесс мониторинга для контроля и управления правами доступа, предоставляемыми каждому пользователю в системе, либо отзываемыми у пользователя.
5. Запросы на доступ не должны быть основаны на зеркальном дублировании или клонирование прав другого пользователя. Запросы должны указывать явные роли и права с обоснованием в рамках бизнес-структуры, чтобы не допустить расширения привилегий и обеспечить минимально возможные привилегии.

17.16 Идентификация и аутентификация пользователей

До начала сессии или операции, во время которой пользователь может получить доступ к информации Citi, все Системы Поставщика, содержащие конфиденциальную информацию, должны провести аутентификацию пользователя или системы, посредством которой осуществляется доступ.

1. Пользователи должны быть уникально идентифицированы или сопоставлены с технологической платформой с помощью ID пользователя.
2. Проверка подлинности пользователей должна осуществляться на технологической платформе посредством утвержденного метода проверки подлинности. Для ознакомления с текущими утвержденными методами проверки подлинности поставщик должен обратиться к своему основному контактному лицу в бизнес-структуре.

3. Любое использование инфраструктуры совместной аутентификации (например, единый вход, сокращенный вход и другие службы совместной аутентификации) должно соответствовать требованиям Citi к аутентификации (о действующих утвержденных методах Поставщик может узнать у основного контактного лица (BAO)).
4. Данные проверки подлинности личности (IVD), используемые для аутентификации пользователя в информационной системе, должны быть зашифрованы при передаче и хранении. Требования к шифрованию см. в разделе 17.9.
5. Каждый счет, используемый сотрудниками Поставщика для доступа к системам Citi, должен быть сопоставлен с уникальным идентификатором, назначенным Citi (например, GEID). Универсальные или общие идентификаторы пользователей для пользователей-людей запрещены, чтобы обеспечить возможность отслеживать происходящее, применение SOD и готовность к аудиту.

17.17 Идентификация лиц с привилегированным доступом и временный привилегированный доступ

Поставщик должен вести реестр всех идентификационных данных и выявлять лиц, имеющих привилегированный доступ или доступ к электронным хранилищам (массивам данных или базам данных, поддерживающим приложения бизнес-структуры), которые содержат информацию, классифицируемую как конфиденциальная информация, которая позволяет установить личность, или более секретная информация. Поставщик должен внедрить средства контроля, защищающие от несанкционированного использования этих идентификаторов. Если работнику требуется доступ к привилегированному идентификатору или к электронным хранилищам, о которых говорилось выше, доступ должен быть предоставлен в рамках процесса управления временным доступом, при котором:

1. лицо, подавшее запрос, должно быть внесено в список предварительно одобренных авторизованных пользователей или получить разрешение во время использования;
2. требуется документированное обоснование в заявке на изменение / решение проблемы до предоставления доступа;
3. проводится независимая проверка активности, осуществленной с доступом;
4. Включает в себя процесс инициирования отзыва или аннулирования доступа в конце срока предоставления временного доступа.
5. в целях стабилизации работы и в период после развертывания (например, после крупного обновления, поломки и устранения проблемы) допускается продление доступа на период до семи (7) календарных дней.

17.18 Проверка прав доступа пользователей

1. Поставщик должен внедрить документированный процесс проверки, подтверждения и удаления прав доступа пользователей к Системам, содержащим конфиденциальную информацию и используемым для

хранения, обработки, управления и/или передачи информации Citi, по крайней мере, раз в полгода.

2. Пользователям запрещается проверять или утверждать свои собственные права или права лица, которое делегировало им полномочия на проверку.
3. После изменения функции сотрудника Поставщика внутри Citi, у Поставщика есть 14 календарных дней на выполнение проверки доступа и прав и удаление доступа к данным Citi, если они больше не требуются сотруднику для выполнения его новой функции.

17.19 Безопасные процедуры входа в систему

1. Заблокированные идентификаторы пользователя должны быть повторно включены с помощью стандартного для отрасли сервиса сброса или другой авторизованной функции. Баннерный текст, если он поддерживается операционной системой или приложением, должен отображаться во всех точках входа в сеть, где пользователь первоначально регистрируется или проходит аутентификацию.

17.20 Система управления паролями

1. Статические пароли пользователей ни при каких обстоятельствах не должны отображаться на экране открытым текстом. Функция переключения видимости пароля исключается из этого требования при соблюдении следующих условий:
 - (1) Ввод пароля маскируется по умолчанию.
 - (2) Видимость пароля может быть инициирована только в результате явных действий пользователя.
 - (3) Пароль повторно маскируется автоматически в течение максимум 15 секунд после того, как пользователь прекращает выполнять действие.
2. Пароли привилегированных функциональных идентификаторов не должны быть закодированы открытым текстом.
3. Статические пароли должны состоять как минимум из десяти (10) буквенно-цифровых символов с учетом регистра. При каждой проверке подлинности следует подтверждать чувствительность регистра для статических паролей. Статические пароли функциональных идентификаторов (FID) должны содержать как минимум 15 знаков для приложений, выпущенных после 31 августа 2026 г.
4. PIN-коды могут использоваться в качестве единственного метода аутентификации для доступа к информационным системам только в том случае, если PIN-код необходим для соблюдения ограничений физического устройства (например, клавиатуры, телефона, смарт-карты).
5. Все статические пароли необходимо менять как минимум каждые 90 календарных дней.
6. Все статические пароли должны блокироваться после максимум шести (6) подряд неудачных попыток входа в систему или шести (6) подряд попыток выполнить сброс пароля. Пароли подлежат разблокированию через функцию ID администратора или автоматической разблокировке не менее чем через 30 минут.

7. Все системы аутентификации должны обеспечить контроль за неактивностью/неиспользованием входа в систему в течение не более 100 календарных дней. Если это технически осуществимо, отключенные логины могут быть повторно включены пользователем или другой уполномоченной функцией.
8. Процесс аутентификации должен обеспечить невозможность повторного использования одного из по меньшей мере шести (6) старых паролей.

17.21 Использование системных утилит

Поставщик обязан ограничить использование служебных программ, позволяющих обойти средства контроля системы и приложений (например, путем загрузки с периферийных устройств), и внедрить соответствующие меры контроля.

17.22 Истечение времени сеанса

1. Вход в систему и повторная аутентификация должны осуществляться для всех пользователей Системы, содержащей конфиденциальную информацию и используемой для хранения, обработки и/или передачи информации Citi.
2. Пользователи должны проходить повторную аутентификацию после периода бездействия, не превышающего 30 минут. Активность включает любой ввод данных на конечной точке (мышь, клавиатура, сенсорный экран и т. д.). В тех случаях, когда управление осуществляется с помощью защищенной паролем экранной заставки, использование приложений / единого входа не требуется.

17.23 Прекращение прав доступа пользователей

1. После освобождения сотрудника от должности или увольнения, доступ или права пользователя, которые могут обеспечить доступ к конфиденциальной информации Citi или информации более высокого уровня защиты (включая логин пользователя для входа на Рабочий стол / в Активную директорию, для единого входа в систему (SSO), электронную почту, токены одноразового пароля (OTP) и удаленный доступ), подлежат немедленному удалению.
2. Если сотрудник имеет доступ к системам, принадлежащим Citi и управляемым ею, об изменении функции или увольнении сотрудника необходимо немедленно уведомить менеджера по деловым отношениям Citi, BAO или поддержку BAO, чтобы менеджер бизнес-структуры Citi инициировал закрытие доступа для уволенных сотрудников к дате прекращения их работы.
3. Поставщик имеет документированный процесс восстановления доступа ко всем активам в соответствии со сроками, указанными в разделе 17.23.2, когда сотрудник или лицо, не являющееся сотрудником, складывает свои полномочия или подвергается увольнению.
4. При обнаружении Поставщиком каких-либо аномалий в отношении пунктов 17.23.1–17.23.3 Поставщик должен незамедлительно уведомить

менеджера по деловым отношениям Citi, BAO или поддержку BAO, предоставив разумное обоснование и средства контроля.

17.24 Удаленный доступ

Поставщик должен предусмотреть средства управления удаленным доступом для защиты доступа к сетям, которые могут хранить, обрабатывать или передавать конфиденциальную информацию Citi или информацию более высокого уровня защиты, включая:

1. Удаленный доступ к информационным системам, используемым для хранения, обработки, управления и/или передачи информации Citi, должен быть защищен от несанкционированного использования.
2. На всех ноутбуках и стационарных компьютерах, находящихся в ведении Поставщика и используемых для хранения, обработки и/или передачи информации Citi, на которых доступ к локальному хранилищу или центру обработки конфиденциальной информации или информации более высокого уровня защиты осуществляется удаленно, должно быть включено шифрование при помощи средства шифрования, соответствующего отраслевым стандартам.
3. Удаленное соединение следует устанавливать исключительно с помощью одобренных решений для удаленного доступа, которые используют многофакторную аутентификацию (MFA).
4. При прямом подключении к сети Интернет вычислительных систем Поставщика на них должен быть установлен индивидуальный брандмауэр (т. е. не посредством брандмауэра или прокси-сервера, находящихся под управлением поставщика).
5. Устройства, находящиеся под управлением Поставщика, должны регулярно подключаться к сети Поставщика, чтобы получать и устанавливать регулярные обновления ПО/антивирусных инструментов, что является условием для получения полного доступа к сети. В целях обновления устройства допускается получать ограниченный доступ.
6. Если для доступа к конфиденциальной информации Citi или информации более высокого уровня защиты используются устройства, не принадлежащие Поставщику и не управляемые им, они должны использовать авторизованное решение, которое не позволяет загружать данные на локальный компьютер. Должны быть приняты следующие меры контроля:
 - a) Запрет на загрузку данных Citi на устройство, не входящее в управляемое компанией решение.
 - b) Поставщик должен обеспечить безопасность такого доступа с помощью аутентификации на основе токенов или сертификатов с использованием стандартных технологий удаленного доступа (например, Virtual Desktop Interface (VDI)).
 - c) Решения для удаленного доступа, в частности, Terminal Services и VMware Horizon, должны быть настроены для отключения общего доступа к буферу обмена и сопоставления дисков по протоколам Blast, PCoIP и для отключения протоколов RDP и SSH.

7. Если для MFA используются программные токены, например, для доступа к программному приложению на мобильном устройстве, программное обеспечение для аутентификации программных токенов должно подтвердить подлинность пользователя (например, с помощью пароля, биометрической идентификации и т. д.) и предотвратить использование программных токенов, если мобильный телефон был взломан или к нему был получен доступ с полномочиями суперпользователя (используется операционная система, отличная от сертифицированной и предоставленной поставщиком мобильного устройства).
8. Весь персонал Поставщика (включая, помимо прочего, постоянных/временных сотрудников, подрядчиков и субподрядчиков, которым требуется особый, привилегированный и/или административный доступ к системам, хранилищам данных, приложениям и/или инфраструктуре, в том числе, помимо прочего, системные администраторы, администраторы баз данных, администраторы контроля доступа, администраторы брандмауэров, администраторы веб-сайтов и т. д.), прямо или косвенно связанный с Услугами, предоставляемыми Citi, должен использовать только многофакторную аутентификацию (MFA), причем такой доступ будет независимо регистрироваться и контролироваться Поставщиком на предмет подозрительной деятельности и/или несанкционированного доступа в соответствии с данными Требованиями.
9. Для персональных устройств и устройств, принадлежащих третьему лицу, поставщик должен иметь эффективное решение для обеспечения того, чтобы такие устройства имели утвержденную версию операционной системы, патчи, антивирусные программы и средства защиты от вредоносного ПО, прежде чем таким устройствам будет разрешено входить в сеть.
10. Поставщик должен гарантировать соблюдение всем его персоналом следующих правил:
 - a) Наличие уединенного отдельного рабочего места, которое не содержит никаких голосовых помощников (например, Siri или Alexa), устройств видеозаписи и/или любых других устройств для воспроизведения/записи фотографий, видео или аудио. Неуполномоченному персоналу не разрешается просматривать какие-либо данные, системы и приложения, которые могут появиться на экранах удаленных вычислительных систем.
 - b) Блокировать вычислительное устройство, если оно оставляется без присмотра, чтобы обеспечить надлежащее предотвращение несанкционированного доступа к просмотру экрана.

17.25 Правило чистого стола

Сотрудники Поставщика обязаны защищать информацию Citi во всех формах, в том числе информацию на материальных носителях, которая используется или хранится на их рабочем месте. От Поставщиков требуется доводить это

требование до сведения всех своих сотрудников не реже, чем раз в год в рамках мероприятий по обучению ИБ или по другому каналу.

17.26 Пожарная безопасность

1. Поставщик должен соблюдать применимые юридические и нормативные требования, регулирующие физическую безопасность и создание безопасной рабочей среды, включая местные пожарные нормы.
2. Поставщик должен использовать системы обнаружения пожара, сигнализации и пожаротушения. Системы должны проверяться каждые полгода и ежегодно тестироваться.

17.27 Физическая охрана

1. Данные Citi должны храниться в охраняемых местах, оборудованных средствами контроля, позволяющими осуществлять доступ в эти места только уполномоченным сотрудникам.
2. Поставщик должен иметь документированную и проверяемую систему контроля физического доступа.
3. Поставщик должен использовать сочетание систем охранной сигнализации / охранных систем, которое включает охранную сигнализацию, контролируемую третьим лицом, охранников и видеонаблюдения, в зависимости от условий и предоставляемых услуг.
4. Поставщик должен иметь документально оформленную политику в отношении посетителей, включающую требование о предоставлении всеми посетителями удостоверения личности по прибытии, входе и выходе.

17.28 Процедуры оперативной безопасности и ответственность

1. Процесс управления изменениями у Поставщика должен включать в себя ключевые контрольные точки, связанные с регистрацией, проверкой, тестированием, утверждением, внедрением и закрытием изменений. Поставщик должен также иметь процесс экстренного внесения изменений, требующий включения иерархии обязательных согласований на всех перечисленных выше этапах.
2. Поставщик должен иметь поддающийся проверке процесс управления мощностями, который включает в себя (помимо прочего) индикаторы/показатели доступности, мощности и производительности; оценку влияния на бизнес-деятельность; проактивное отслеживание, расследование и устранение проблем с производительностью и мощностями.
3. Если это возможно, Поставщик обязан физически и/или логически отделить среды лаборатории, разработки, тестирования и производства друг от друга.

17.29 Требования к разработке программного обеспечения

Применяются к Поставщикам, предоставляющим программное обеспечение, предназначенное для использования только компанией Citi. Поставщики должны соблюдать эти требования или продемонстрировать документально зафиксированный и утвержденный процесс жизненного цикла разработки

программного обеспечения (SDLC) с эквивалентным подходом равноценного качества.

17.30 Инициирование и планирование

Поставщик должен определить объем и цели решения в соответствии с требованиями и договорными обязательствами Citi. Сюда входит следующее:

1. Документальная фиксация функциональных и нефункциональных требований.
2. Предоставление оценки трудозатрат и сроков выполнения работ.
3. Определение всех сторонних компонентов или зависимостей.

Действия по обеспечению соблюдения данных требований и обязательств, включая оценку риска безопасности, должны быть инициированы в самом начале проекта. Следует четко проинформировать о ролях, обязанностях и контрольных точках утверждения.

Все среды должны быть классифицированы как среда разработки (DEV), среда тестирования (TEST) или среда производства (PROD), и они должны оставаться строго отделенными друг от друга на протяжении всего жизненного цикла. Классификация среды определяет разрешения доступа и тип данных, которые могут обрабатываться. Поставщик должен ограничить доступ на основании определения среды и привести развертывание решения в соответствии с соответствующим завершением этапа SDLC, чтобы предотвратить несанкционированный доступ или нарушение безопасности данных.

17.31 Разработки

Поставщик должен документально зафиксировать подход к разработке, который обеспечивает соответствие поставляемого решения всем заявленным требованиям (далее — «План тестирования»). План тестирования должен включать в себя и описывать, как минимум, следующее:

1. все тесты, которые должны быть выполнены командой разработчиков, включая модульные, функциональные и нефункциональные тесты, а также тесты аспектов производительности, с возможностью отслеживания соблюдения требований;
2. определение утверждающего лица, которое должно подтвердить выполнение тестов;
3. требования к тестированию безопасности, такие как оценка уязвимости и моделирование угроз; и
4. среда, подход, процесс и путь поддержки тестирования.

Необходимо подготовить стратегию выпуска решения с описанием предпосылок и процесса выпуска решения в среду TEST и PROD, включая критерии готовности выпуска, контент и темпы поставки на протяжении всего жизненного цикла проекта.

Если в Договоре указано такое требование, распределение программного обеспечения должно осуществляться в утвержденном компанией Citi формате с использованием утвержденных компанией Citi инструментов и рабочих процессов.

17.32 Тестирование

Тестирование должно быть запланировано и проведено в контролируемой среде, чтобы подтвердить, что решение соответствует определенным требованиям и критериям успешного создания. Случаи тестирования должны иметь прослеживаемую связь с требованиями и коммитами кода.

Поставщик должен подготовить отчет, содержащий краткую информацию о результатах успешного или неудачного прохождения тестирования, дополнительном тестировании, проведенном в ходе разработки, и тестированиях, которые не были выполнены (с указанием причин) («Отчет о завершении тестирования»). Необходимо документально зафиксировать недостатки и отложенные на будущее возможности, а также планы устранения нерешенных проблем.

По запросу Citi Поставщик должен предоставить доказательства следующих компонентов:

1. подробный план тестирования;
2. выполнение тестирования и результаты, описанные в отчете о завершении тестирования; и
3. прослеживаемая связь результатов тестирования с требованиями и коммитами кода.

17.33 Развертывание

Перед развертыванием Поставщик должен выполнить все необходимые тестирования безопасности, включая проверку уязвимостей и моделирование угроз. Процесс выпуска должен иметь структуру, включающую в себя документально оформленные записи об изменениях, стратегии возврата и необходимые согласования. Планы внедрения и инструкции по развертыванию должны включать в себя протоколы мониторинга и эскалации.

После развертывания Поставщик должен окончательно утвердить идентификаторы системы и обновить все соответствующие объекты, чтобы обеспечить готовность к проверке.

17.34 Безопасность

1. Структурированная оценка, проведенная на этапе разработки SDLC для выявления и устранения возможных рисков безопасности, уязвимостей и архитектурных недостатков до создания кода («Проверка разработки в отношении безопасности»), должна быть включена в SDLC со средствами контроля, отвечающими за предупреждение и выявление рисков, которые соответствуют отраслевым стандартам, таким как OWASP.
2. Необходимо соблюдать правила безопасного кодирования.
3. Поставщик обязан внедрить средства контроля за информационной безопасностью в свои процессы и процедуры выбора, разработки и развертывания приложений, продуктов и услуг.
4. Поставщик должен иметь процедуру обеспечения безопасности для всех систем, в которых хранится и обрабатывается информация Citi и (или) посредством которых осуществляется передача информации Citi, а также он должен иметь в своем распоряжении безопасный образ или шаблон для всех систем.

17.35 Средства защиты от вредоносных программ

Поставщик должен внедрить средства контроля для предотвращения и обнаружения внедрения вредоносного кода (например, вирусов, червей, троянских программ, рекламного и шпионского ПО, программ-вымогателей или других подобных кибератак, при которых данные могут быть скомпрометированы). Поставщик обязан:

1. Внедрить, обновить и поддерживать технологии противодействия вирусам и шпионскому ПО на всех персональных компьютерах и технологии на всех серверах локальной сети (LAN), почтовых серверах и прочих устройствах, на которых хранится, обрабатывается и/или посредством которых осуществляется передача данных Citi.
2. Предусмотреть настройки безопасности, не позволяющие конечным пользователям отключать антивирусные программы / средства защиты от вредоносного ПО и плановые сканирования.
3. Предусмотреть централизованно управляемые автоматизированные процедуры настройки и обновления антивирусных программ и программ защиты от вредоносного ПО.
4. Обеспечить реализацию процедур идентификации и адресации компьютеров, не соответствующих требованиям, на которых установлены устаревшие антивирусные сигнатуры или антивирусные ядра.
5. Контролировать доступ к портам/интерфейсам связи, которые позволяют подключаться к внешним устройствам, включая, помимо прочего, носители информации.

17.36 Средства контроля использования мобильного кода

Поставщики должны обеспечить внедрение средств контроля, обеспечивающих безопасность мобильного кода. Когда использование мобильного кода разрешено, конфигурация должна, как минимум, соответствовать всем применимым отраслевым стандартам и договорным обязательствам перед Citi, а Поставщик должен обеспечить работу разрешенного к использованию мобильного кода в соответствии с четко определенной и документально зафиксированной политикой безопасности и предотвращать выполнение мобильного кода, использование которого не было разрешено.

Если мобильный код может повлиять на основную операционную систему или платформу (т. е. если он расположен вне контролируемой среды), Поставщик обязан обеспечить выполнение следующих условий:

1. Мобильный код, опубликованный Поставщиком, должен быть подписан одобренным Citi центром сертификации; Поставщик обязан отслеживать сертификат на протяжении всего жизненного цикла для своевременного продления срока его действия.
2. Подписанный мобильный код с сертификатом, срок действия которого истек, должен быть удален из производственной среды.

17.37 Введение контрольных журналов

Поставщик должен убедиться, что все системы, содержащие конфиденциальную информацию и используемые для доступа, хранения, обработки и/или передачи данных Citi, ведут журналы регистрации событий на уровне инфраструктуры или приложений для записи перечисленных ниже событий:

1. Действия, связанные с безопасностью инфраструктуры соответствующей платформы
2. Все аварийные сигналы системы, связанные с событиями безопасности, сгенерированными брандмауэром или IDS/IPS
3. Все попытки нарушения безопасности системы (например, неудавшиеся попытки входа пользователя в систему)
4. Несанкционированные попытки доступа к ресурсам (программному обеспечению, данным, процессам и т.д.)
5. Действия администратора
6. Информация, связанную с получением конкретной информации от пользователя или другой системы
7. Все крупные события, связанные с финансовыми операциями и информацией Citi, в частности, следующие:
 - a. Обновления финансовых транзакций
 - b. Обновления конфиденциальной и секретной информации, которая позволяет установить личность (PII)
 - c. Обновления данных с ограниченным доступом
 - d. Обновления данных для аутентификации
8. Все установленные сеансы.
9. Когда это позволяют технические средства, в целях содействия расследованию случаев мошенничества в приложениях, обращенных к Citi (на веб-сайтах и в мобильных приложениях), требуется регистрировать артефакты сеанса, например, уникальный идентификатор устройства. Эти артефакты должны как минимум содержать IP-адреса. Эти артефакты должны быть зафиксированы для транзакций Citi и активности по открытию счета Citi. Информацию следует собирать таким образом, чтобы можно было установить связь артефакта сеанса с операцией или открытием счета.
10. В журнале регистрации событий должно быть задокументировано назначение конкретного действия конкретному физическому лицу, чтобы предотвратить отказ от ответственности.
11. Необходимо регистрировать значительные события, связанные со службой информационной безопасности (ISA), в том числе следующие:
 - a) Создание пользователя
 - b) Изменение прав доступа пользователей
 - c) Удаление, создание, модификация профилей в системах, содержащих конфиденциальную информацию
 - d) Восстановление паролей
 - e) Изменения конфигурации системной безопасности
 - f) Вся интерактивная активность привилегированных функциональных ID

- g) Журналы безопасности должны содержать по крайней мере следующую информацию независимо от системы генерирования журнала, если такое включение технически возможно:
- I. Дата и время события (время в формате UTC)
 - II. ID пользователя лица, выполняющего действие
 - III. Тип события
 - IV. Название затронутых активов или ресурсов
 - V. Тип доступа (удалить, изменить и т.д.)
 - VI. Успех или неудача события
 - VII. Источник (терминал, порт, местонахождение, IP, имя узла и др.)

17.38 Защита информации в журналах

Поставщик должен обеспечить внедрение средств контроля доступа для сохранения целостности журналов регистрации событий во время начала их ведения, после завершения их ведения, в период их хранения и в момент передачи.

1. Для предотвращения несанкционированного изменения контрольных журналов Поставщик должен защитить журналы от перезаписи или изменения пользователями, действия которых эти журналы отслеживают.
2. Поставщик обязан предоставить Citi процедуру хранения документов, определяющую порядок хранения данных журнала регистрации событий и включающую меры по обеспечению соблюдения нормативно-правовых требований со ссылками на все применимые законодательные и нормативно-правовые требования.
3. Часы систем обработки информации и доменов безопасности в организации должны синхронизироваться с надежным источником времени.

17.39 Контроль использования системы

Поставщики должны обеспечить, чтобы следующие события отслеживались, регистрировались в журнале и проверялись путем ручной или автоматической проверки:

1. Все системные оповещения, связанные с событием безопасности, созданным брандмауэром или системой обнаружения проникновения (IDS) / системой предотвращения проникновения (IPS).
2. Все обновления критически важных ресурсов, перечисленные в стандартной сборке.
3. Все интерактивные действия, выполняемые любыми идентификаторами (функциональными, привилегированными, системными, временными и т. д.) с доступом к информации, классифицируемой как конфиденциальная информация, позволяющая установить личность, или информация более высокого уровня защиты.
4. Значительные события ISA, перечисленные в разделе «Ведение контрольных журналов» выше, со следующим исключением:

- а) Отмена полномочий пользователя, роли или профиля в случаях, если функция управления информационной безопасностью выполняется автоматизированным рабочим процессом/автоматической системой с непрерывным контролем целостности данных.

17.40 Согласование и проверка журналов

1. Если событие, регистрируемое в журнале, активирует предупреждение, а событие анализируется, Поставщик должен инициировать необходимые действия, а при наличии признаков потенциально опасного происшествия в области информационной безопасности, провести расследование.
2. Поставщик должен обеспечить внесение журналов аудита в центральную систему управления журналами, такую как Security Information and Event Management (SIEM), или в инструмент анализа журналов, для анализа и проверки согласования журналов.
3. Поставщики должны периодически проверять и корректировать параметры своей системы SIEM или инструмента для анализа журналов, чтобы повысить качество выявления событий, требующих принятия мер.

17.41 Контроль служебного программного обеспечения

Поставщик должен гарантировать, что он использует только операционные системы и программное обеспечение, поддержку которых в настоящее время осуществляет общепризнанный в отрасли поставщик коммерческих решений либо к которым активно и должным образом выпускаются актуальные изменения и обновления конфигураций для устранения угроз безопасности.

Поставщик должен обеспечить внедрение документально зафиксированного процесса, в котором указаны сроки устранения проблем, в течение которых должны быть применены все утвержденные исправления и параметры системы безопасности.

Независимо от наличия любых отдельных соглашений об обслуживании между Поставщиком и Citi, Поставщик должен обеспечить, чтобы программное обеспечение, разработанное для Citi и регулируемое лицензионным соглашением, не разрешало использовать неподдерживаемые версии программного обеспечения, имеющие известные уязвимости, и чтобы такое программное обеспечение надлежащим образом и своевременно получало обновления и исправления.

Прикладное программное обеспечение, используемое для обработки информации Citi, должно быть приобретено у официальных поставщиков, оно должно быть лицензированным, и его следует внести в каталог программного обеспечения компании, а поставщик должен обеспечить для него техническую поддержку.

17.42 Управление уязвимостями и угрозами

1. Поставщик должен внедрить процесс управления уязвимостями и угрозами, который всесторонне прорабатывает и/или включает все нижеперечисленное:
 - a. Инструменты и процедуры для обнаружения уязвимостей во всех активах, которые могут использоваться для обработки, хранения, доступа или передачи конфиденциальной информации Citi или более чувствительной информации, и управление этими уязвимостями.
 - b. Требование проводить проверку не реже одного раза в неделю с использованием признанных в отрасли инструментов выявления уязвимостей и методов составления отчетности.
 - c. Рейтинг уязвимостей в соответствии с наиболее актуальной версией Общей системы оценки уязвимостей (CVSS) (см. <https://www.first.org/cvss>) с указанием сроков устранения в зависимости от степени серьезности.
 - d. Требование тестирования исправлений для уязвимостей перед полным производственным развертыванием.
 - e. Документированный и повторяющийся рабочий процесс ускорения устранения важнейших уязвимостей.
 - f. Поставщик должен отслеживать активы на протяжении всего поддерживаемого жизненного цикла, чтобы подготовиться к окончанию срока службы (EOL) или окончанию срока поддержки поставщиком (EOVS), и разработать процессы предупредительного обновления или замены таких активов.
 - g. Любые критические уязвимости системы оценки CVSS, выявленные с помощью сбора данных, проверки уязвимости или испытания на проникновение, должны быть устранены в приоритетном порядке в четко определенные сроки, соразмерные риску уязвимости.

17.43 Приложения, хостинг для которых предоставляется Третьими лицами

Если Поставщик поддерживает или хранит Конфиденциальную информацию Citi или более чувствительную информацию на веб-сайте или в системе, доступной в Интернете, или на сайте под брендом Citi, то для защиты от уязвимости или угрозы, связанной с продуктами или услугами, влияющими на Citi (далее «Уязвимость»), Поставщик должен соблюдать следующие Требования:

1. Назначить одного сотрудника Поставщика для ответа на запросы Citi в отношении информационной безопасности.
2. Применять признанные в отрасли наилучшие решения для не менее, чем еженедельного мониторинга авторитетных источников информации об уязвимостях компьютерной безопасности, таких как FIRST, CERT/CC, CISA Known Exploited Vulnerabilities Catalog и списки рассылки поставщиков, и принимать соответствующие меры для получения, тщательного тестирования, применения и предоставления Citi

соответствующих пакетов сервисов, патчей, обновлений и обходных путей.

3. Не реже одного раза в квартал тестировать реализацию своих мер информационной безопасности с использованием инструментов сканирования уязвимостей сети, системы и приложений и/или тестирования на проникновение.
4. Разрешить Citi или утвержденной Citi третьей стороне проводить через обоснованные промежутки времени оценку уязвимостей, оценку испытаний на взлом и другие оценки безопасности, чтобы проверить соблюдение Поставщиком своих обязательств по любому договору и настоящим Требованиям, в том числе, помимо прочего, проверку политик, процессов и процедур, оценку мер физической безопасности на объекте компании, анализ уязвимостей сетей, систем и приложений, а также испытание на проникновение с использованием доступных на рынке инструментов и (или) стандартных для отрасли методов проведения таких оценок и проверок.
5. Любой подрядчик, предоставляющий Поставщику услуги по оценке уязвимости, должен выбираться из утвержденного Citi списка поставщиков услуг по оценке уязвимости. Если Поставщик использует подрядчиков или субподрядчиков для предоставления Услуг, Поставщик должен за свой счет обеспечить, чтобы любые требуемые оценки уязвимостей, выполнялись так же своевременно, как если бы Поставщик предоставлял эти Услуги напрямую, и должен гарантировать, что данное требование зафиксировано в соглашении между Поставщиком и подрядчиком/субподрядчиком, касающемся Услуги, включая формулировки, разрешающие Citi проводить такие оценки.
6. **Уведомление.**
 - a) Если Поставщик обнаружит уязвимость, связанную с продуктом или услугой и влияющей на Citi, Поставщик должен уведомить Citi об этом в письменной форме в течение 24 часов с момента обнаружения и приложить описание мер по исправлению положения, предпринимаемых Поставщиком.
 - b) Если Поставщику станет известно об уязвимости, связанной с продуктом или услугой и влияющей на Citi, после ответственного публичного раскрытия информации по технологическим каналам (публикация уязвимости в Национальной базе данных уязвимостей (NVD) или через каталог угроз, предоставленный внешним поставщикам средств обеспечения безопасности), Поставщик уведомит об этом Citi в письменной форме в течение 24 часов с момента такой публикации. Каждое уведомление будет включать в себя информацию об уязвимости, информацию системной служебной программы об услугах, относящихся к Citi (т. е. используется ли в ней информация Citi, используется ли она при предоставлении услуг, или используется ли в ней информация Citi и используется ли она при предоставлении услуг одновременно), информацию о том, может ли она быть

использована удаленно, и оценку общих уязвимостей и воздействий (CVE). Поставщик обязуется продолжать предоставлять обновления Citi до устранения уязвимости. В случаях, когда уязвимость выявляет Citi, Citi может уведомить об этом Поставщика; при этом Поставщик должен незамедлительно устранить Уязвимость в соответствии с настоящим разделом.

7. **Исправление.** Для каждой Уязвимости, описанной в настоящем разделе, уведомляющая Сторона будет оценивать уровень риска и влияние такой уязвимости на основе серьезности и риска для Citi и назначать уровень приоритета риска на основе Общей системы оценки уязвимостей (CVSS), как указано в Приложении А к этому документу (см. <https://www.first.org/cvss>). Как только уровень риска будет назначен и согласован сторонами, Поставщик обязуется устранить любую выявленную уязвимость со средним, высоким или критическим уровнем риска. По возможности, исправление любой такой уязвимости предоставляется в пакете безопасности для текущей развернутой версии.

Если Поставщик не может или не желает устранить уязвимость удовлетворительным для Citi образом, Citi может прекратить действие соответствующей лицензии без какой-либо дополнительной ответственности или финансовых обязательств (для части, действие которой было прекращено), при этом Поставщик должен незамедлительно возместить Citi пропорциональную часть уплаченных лицензионных сборов.

17.44 Средства управления сетью безопасности коммуникаций

1. Сети Поставщика, используемые для доступа, хранения, обработки, управления и/или передачи информации Citi, необходимо защитить от угроз, а для информационных систем, подключенных к сети, требуется предусмотреть средства обеспечения безопасности в рамках узлов применения принудительной защиты в сети.

- a. Информацию, отнесенную к категории конфиденциальной или более высокого уровня защиты, запрещено постоянно хранить в системе, подключенной к демилитаризованной зоне (DMZ) с выходом в Интернет. Сети, используемые для доступа, хранения, управления, обработки и/или передачи информации Citi с использованием беспроводных локальных сетей (WLAN) или других беспроводных устройств, которые включают в себя разумные средства контроля для запрещения несанкционированного доступа (PEAP-TLS, EAP-TTLS и т.д.), могут быть подключены к сетям, содержащим информацию Citi.
 - b. Все внешние IP-подключения к глобальной сети Поставщика должны быть защищены брандмауэром, находящимся под контролем Поставщика.
 - c. Необходима система обнаружения вторжений (IDS) и система предотвращения вторжений (IPS), которая в реальном времени контролирует и защищает Интернет-соединения с сетью Поставщика в сети, используемой для доступа, управления, хранения, обработки или передачи информации Citi.
2. Для всех интернет-приложений под торговой маркой Citi Поставщик должен обеспечить следующее:
- a. Сервисы, размещенные на сайтах Поставщика, защищены от DDoS-атак (распределенных атак типа «отказ в обслуживании») одобренными Citi решениями или аналогичными средствами контроля, прошедшими проверку Citi.
 - b. Внешние брандмауэры должны быть настроены с правилом отказа по умолчанию. Правила брандмауэра должны быть настроены таким образом, чтобы предоставлять пользователям минимально необходимый уровень доступа и отклонения любых попыток соединений брандмауэром (например, отбрасывание пакетов) подлежат внесению в журнал/документированию.
 - c. Отмена сетевого трафика связи производится по умолчанию, а разрешение осуществлять сетевой трафик связи производится в качестве исключения в рамках управляемых интерфейсов. Исключения должны быть строго ограничены конкретными источниками, пунктами назначения и услугами.
 - d. Трафик веб-приложений должен иметь надлежащие средства контроля, и его следует фильтровать, например, через брандмауэры веб-приложений.

17.45 Разделение в сетях

Поставщик должен убедиться, что доступ ко всем информационным системам и приложениям, используемым для доступа к информации Citi, а также для хранения, обработки, администрирования и (или) передачи информации Citi, и доступ к которым осуществляется через Интернет, осуществляется через демилитаризованную зону Поставщика (DMZ).

В случае возникновения чрезвычайных происшествий Поставщик должен иметь возможность ограничить доступ к разным частям сети, чтобы снизить сетевую

угрозу от событий, связанных с безопасностью (например, фильтрация портов во время поражения вирусом).

Система защиты удаленного доступа и хост-узла должна использовать средства контроля за доступом на основании групп (например, сотрудники, субподрядчики), чтобы ограничить доступ к сетевым ресурсам в сети Поставщика. На уровне хост-узла контроль за доступом может осуществляться на уровне группы или отдельного лица.

17.46 Идентификация оборудования в сетях

Технологические платформы должны выявлять и проверять подлинность одноранговых технологических платформ в соответствии с уровнями риска информационной безопасности средств контроля за взаимодействием и средств контроля, ориентированных на снижение рисков.

1. Для доступа к сети Поставщика, где хранится, обрабатывается или передается информация Citi, могут использоваться только устройства Поставщика (т. е. оборудование, включая, помимо прочего, настольные ПК и ноутбуки), соответствующие настоящим требованиям и разрешенные Поставщиком.
2. Для доступа к сети Citi могут использоваться только устройства Поставщика (т. е. оборудование (включая, помимо прочего, настольные ПК, ноутбуки, съемные носители информации), соответствующие настоящим требованиям и разрешенные Citi.

17.47 Анализ и описание требований к безопасности

Поставщик обязан внедрить процедуры информационной безопасности в свои процессы и процедуры выбора, разработки и развертывания приложений, продуктов и услуг.

17.48 Онлайн-транзакции

1. Если это возможно, Поставщик должен использовать информационные системы, использующие динамические пароли или цифровые сертификаты для подтверждения регистрационных данных.
2. Все сертификаты для конечных объектов подлежат замене не реже одного раза в 13 месяцев.
3. Приложения поставщика, которые хранят, обрабатывают, управляют или получают доступ к информации Citi, размещают интернет-приложения с фирменным оформлением Citi или имеют подключение к сетевым ресурсам Citi, должны:
 - a. использовать метод проверки подлинности на основании типов данных и функций, к которым осуществляется доступ;
 - b. производить многофакторную проверку подлинности (MFA) и при необходимости выполнять рекомендации;
 - c. проводить оценку адаптации к условиям подозрительной активности (SAM) и при необходимости выполнять рекомендации;
 - d. во всех этих случаях для выяснения актуальных требований Поставщику следует обратиться к основному контактному лицу в Citi.

17.49 Процедуры контроля за изменениями

1. Поставщик обязан производить изменение конфигурации брандмауэров, систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS) посредством процесса управления изменениями Поставщика.
2. Доступ, предоставляемый для производства с помощью временных идентификаторов, подлежит регистрации и мониторингу на предмет отслеживания изменений, внесенных в среду.
3. Для систем, содержащих информацию о клиенте, расцениваемую Citi как конфиденциальную или имеющую более высокую степень защиты, или «Высокое» значение компонента риска ИБ по параметру «Целостность» или «Доступность», журналы, зафиксированные в соответствии с разделом 17.32 («Ведение контрольных журналов»), должны проверяться Поставщиком. Такая проверка может быть основана на соответствующей методологии выборки на основе рисков.
4. Проверка должна установить, что изменения пользователей, получивших временный привилегированный доступ, соответствуют запланированным.
5. Поставщик должен задокументировать все изменения, в том числе хранить доказательства процесса проверки.

17.50 Утечка информации

У Поставщика должен применяться задокументированный Стандарт кодирования для защиты информации, который предотвратит утечку информации, в том числе:

1. Подробная информация о системе (например, тип сервера и технология).
2. Трассировка стека и ошибки исключений, раскрывающие структуру дерева каталогов и тип базовой базы данных.

17.51 Данные проверки

Конфиденциальная информация или информация с более высокой степенью секретности, согласно определениям Citi, не должна использоваться или храниться Поставщиком в средах или лабораториях для разработки или тестирования программных приложений, за исключением случаев, когда эта информация деидентифицируется, маскируется и/или скрывается с использованием инструментов и методов, соответствующих отраслевым стандартам, таким образом, чтобы эти данные больше не являлись чувствительными, или когда Поставщик вынужден использовать те же элементы контроля в продакшн-системе в режиме реального времени, что и в средах разработки или тестирования.

17.52 Приемка системы

Поставщик должен задокументировать существующие процессы управления объемом проекта и принятия системы, соответствующие отраслевым стандартам.

17.53 Отчетность о слабых местах в сфере информационной безопасности

Поставщик обязан принять процесс, в соответствии с которым **Citi будет немедленно получать уведомления** об уязвимостях приложений и инфраструктуры, ставших причиной утечки информационных активов Citi.

17.54 Обязанности и процедуры, связанные с инцидентами безопасности

1. SIRT — это событие в сфере безопасности, которое ставит под угрозу любой из следующих компонентов, независимо от того, как и где произошел инцидент в сфере безопасности, или кто мог его вызвать.
 - Конфиденциальность, целостность или доступность данных компании Citi.
 - Конфиденциальность, целостность или доступность любых данных (включая персональные данные), в отношении которых Citi несет договорные и юридические обязательства, а также обязательства по соблюдению нормативно-правовых требований.
 - Целостность или доступность информационных систем Citi, в которых хранятся, обрабатываются или передаются данные Citi.
2. В наших целях нарушение конфиденциальности относится к предоставлению данных неуполномоченному лицу или к ситуациям, в ходе которых компания Citi перестает хранить данные и теряет контроль над ними. О всех инцидентах в сфере безопасности требуется немедленно сообщать.
3. Если Поставщик столкнулся с SIRT, он должен взаимодействовать с Citi, и в рамках такого взаимодействия он должен предоставить информацию, запрашиваемую Citi в соответствии с собственными процессами реагирования на инциденты Citi, анализировать скомпрометированные данные таким образом, чтобы позволить Citi соблюдать юридические, нормативно-правовые и (или) внутренние требования в отношении управления, предоставить любые или все уведомления, требуемые законом, правилу или нормативно-правовому требованию или необходимые Citi, на дискреционной основе по запросу Citi и за счет Поставщика только после того, как Citi сможет проверить и изменить предлагаемые формулировки шаблонов уведомлений, а Поставщик не должен указывать название Citi в таких уведомлениях, кроме случаев, когда Citi отдельно просит указывать свое название в письменной форме.

17.55 Защита от утечки данных (DLP)

Поставщик должен внедрить средства контроля для предотвращения утечки данных (DLP), включая мониторинг контента и конечных точек, который охватывает всех сотрудников, имеющих доступ к конфиденциальным данным Citi или данным более высокого уровня защиты.

Поставщик должен иметь средства контроля, позволяющие обнаруживать и предотвращать случаи перемещения конфиденциальной информации Citi или информации более высокого уровня защиты за пределы ее сети по следующим каналам:

- a. Незашифрованные электронные письма
- b. Вложения в зашифрованных электронных письмах
- c. Вывод данных Citi на печать
- d. Передача данных Citi за пределы ее сети (например, через FTP)
- e. Попытки скопировать конфиденциальную информацию Citi или информацию более высокого уровня защиты на съемные носители, такие как USB-накопители, съемные жесткие диски, приводы CD/DVD и другие съемные устройства с возможностью хранения данных. Данная привилегия должна быть предотвращена по умолчанию.
- f. Решение DLP должно регистрировать все события, представляющие собой попытки (как успешные, так и заблокированные) переместить, перенести или скопировать конфиденциальную информацию Citi или информацию более высокого уровня защиты из ее сети в другие места, и информировать поставщика о таких событиях. Данная привилегия должна быть предотвращена по умолчанию.
- g. Загрузка данных Citi на внешние веб-сайты, включая сайты SaaS/файлообменники. Данная привилегия должна быть предотвращена по умолчанию.

17.56 Просмотр веб-страниц

1. Поставщик должен иметь средства контроля доступа к Интернету для предотвращения разглашения конфиденциальной информации Citi или информации более высокого уровня защиты, а также для защиты от вредоносного ПО или от атак, направленных на сотрудников, имеющих доступ к данным Citi.
2. Для поставщиков, имеющих доступ к конфиденциальной информации Citi или информации более высокого уровня защиты:
 - a. Все запросы с URL-адресами подлежат регистрации.
 - b. Попытки получить доступ к сайтам, которые могут быть использованы для несанкционированной передачи данных Citi (например, веб-почта, чат, социальные сети, онлайн-хранилище, Gen-AI и т. д.) должны блокироваться.
 - c. Доступ к сайтам, которые могут подвергнуть рабочую среду воздействию вредоносного ПО или атакам, должен блокироваться.

- d. Попытки доступа к сайтам, которые считаются не относящимися к коммерческой деятельности, должны блокироваться.
- e. Поставщик должен подписаться на услугу категоризации URL-адресов с регулярным обновлением; все URL-адреса, которые не были категоризированы, должны блокироваться по умолчанию, или все URL-адреса должны блокироваться по умолчанию и утверждаться в индивидуальном порядке.
- f. Веб-браузеры, используемые Поставщиком, должны поддерживаться в полном объеме, и все последние обновления для системы безопасности, предоставляемые Поставщиком программного обеспечения, должны быть установлены.

17.57 Электронная торговля

Запрещается использовать службы обмена мгновенными сообщениями, одноранговые сети и прочие средства для совместной работы в сети Интернет для передачи или хранения информации Citi за пределами сети поставщика или отправки из сетей, содержащих информацию Citi, если данные Citi не зашифрованы согласно разделу 17.9 («Политика использования средств криптографической защиты информации»).

17.58 Электронная почта

Поставщик должен иметь средства контроля в отношении электронной почты, для предотвращения разглашения конфиденциальной информации Citi, а также для защиты от вредоносного ПО, или от атак. Сюда входит следующее:

1. Файлы, вложенные в электронные письма, поступающие в шлюз электронной почты, сканируются и блокируются в том случае, если они представляют риск для системы.
2. Должно использоваться актуальное программное обеспечение для фильтрации электронной почты (для борьбы со спамом и фишингом).
3. Любая конфиденциальная информация Citi или информация более высокого уровня защиты, отправляемая за пределы организации Поставщика, должна быть зашифрована.
4. Клиентские программы для работы с электронной почтой, используемые поставщиком, должны поддерживаться в полном объеме, все последние обновления для системы безопасности, предоставляемые поставщиком программного обеспечения, должны быть установлены.

17.59 Съёмные носители

1. Поставщик обязан защищать информацию Citi независимо от типа носителя, на котором она хранится. Настоящий стандарт распространяется, помимо прочего, на следующие типы носителей информации: карты, кассеты, компакт-диски (CD), бумага для печати чеков, дискеты и прочие съёмные устройства хранения, информация, которую выводят на физический носитель, магнитные диски, магнитные ленты, микроплёнки, микрофиши, оптические диски и бумажные документы.
2. На системах, в которых хранится информация Citi, по умолчанию должен быть закрыт доступ к портативным носителям / устройствам хранения.

Если предоставляются исключения и таким образом разрешен доступ к чтению и записи, данные должны быть зашифрованы на портативном носителе.

3. Если допускается использование съемных носителей, такое использование должно проходить процедуру утверждения руководством, включая коммерческое обоснование использования съемных носителей. Съемные носители подлежат инвентаризации руководством. Съемные носители, содержащие конфиденциальную информацию Citi или информацию более высокого уровня защиты, подлежат автоматическому шифрованию, не требуя никаких действий от пользователя.

17.60 Уничтожение носителей

1. В случае если информация Citi, отнесенная к категории конфиденциальной информации или информации более высокого уровня защиты, подлежит уничтожению в соответствии с распоряжениями Citi (т. е. она более не нужна / не несет пользы для Citi, а также истек период хранения, требуемый законом, нормативным актом и/или политикой Citi), поставщик обязан уничтожить информацию таким способом, чтобы ее невозможно было восстановить или использовать.
2. Необходимо использовать утвержденный инструмент, который случайным образом перезаписывает секторы диска определенными разными символами, чтобы обеспечить надежное удаление данных со съемных носителей на основе следующих правил:
 - a. Для носителей, на которых хранится информация, классифицированная как конфиденциальная или имеющая более высокий уровень защиты, этот инструмент должен трижды обработать носитель информации.
 - b. Носители подлежат размагничиванию (если применимо).
3. Физически уничтожьте носитель, чтобы сделать его нечитаемым (например, измельчение, разрушение дисков).
4. Бумажные и другие неэлектронные носители информации, содержащие конфиденциальную информацию или информацию более высокого уровня защиты, подлежат безопасному сбору и хранению в надежной «Конфиденциальной корзине» до окончательной утилизации. Конфиденциальные корзины должны быть всегда закрыты, и они могут быть открыты только уполномоченным персоналом.
 - a. Копировальные аппараты, принтеры, факсы и любые другие устройства с памятью или хранилищем данных, которые могут содержать конфиденциальную информацию Citi или информацию более высокого уровня защиты, также подлежат очистке.

17.61 Управление информационной безопасностью и обучение информационной безопасности

1. Вы должны поддерживать соответствующую программу повышения осведомленности и образования в области кибербезопасности и информационной безопасности, которая включает в себя, помимо прочего, предотвращение фишинга и других атак посредством социальной инженерии, надлежащее обращение с конфиденциальной или более секретной информацией, а также составление отчетов об инцидентах в сфере безопасности и управление ответными мерами.
2. Поставщик должен обеспечить прохождение всеми сотрудниками, включая подрядчиков и временный персонал, соответствующего вводного инструктажа и обучения по политикам и процедурам организации, имеющим отношение к их должностным обязанностям.
3. Поставщик должен ежегодно пересматривать и обновлять программу обучения и повышения осведомленности для устранения возникающих рисков и угроз, а также обеспечения применения передовых методов и новых технологий в сфере кибербезопасности.
4. Программа должна включать в себя, как минимум, следующие темы.
 - b. Маркировка и обработка информации
 - c. Безопасная передача информации (защищенная электронная почта, защищенное хранилище SharePoint, запрет на отправку данных, принадлежащих Citi, на личную электронную почту)
 - d. Отчетность о происшествиях в сфере информационной безопасности
 - e. Защищенное рабочее место (например, надлежащее использование Интернета, несанкционированное программное обеспечение, запрет на загрузку неутвержденного программного обеспечения)
 - f. Управление паролями (например, надежные пароли, запрет на предоставление паролей другим лицам)/
 - g. Социальная инженерия (например, фишинг, адресный фишинг, вишинг, смишинг)
 - h. Удаленная работа (например, защищенное и безопасное соединение, безопасность личных устройств)
5. Сотрудники поставщика должны получить задание на прохождение обучения в ходе или до получения доступа к системам, на которых размещаются данные Citi, и они должны пройти обучение к дате, указанной в уведомлении о задании на прохождение обучения.
 - a. Обучение по вопросам IS должно проводиться для всех сотрудников не реже одного раза в год, если это не запрещено законом.
6. Обучение должно включать в себя компонент, позволяющий определить его эффективность (например, проверка знаний после прохождения обучения с пороговым значением, определяющим, успешно или неудачно слушатель прошел обучение), если местное законодательство допускает использования такого компонента.

17.62 Программа управления киберрисками

Поставщик также должен, как минимум, внедрить соответствующую программу управления киберрисками, которая включает, как минимум, следующее:

1. Поддерживать четко определенную, задокументированную программу управления рисками информационной безопасности и/или программу управления операционными рисками, которая имеет четко определенный компонент управления кибер/информационными рисками, определяющий уровень толерантности Поставщика к киберрискам и гарантирующий, что его остаточный киберриск совпадает с уровнем толерантности.
2. Поддерживать надлежащую программу управления рисками безопасности, которая включает, помимо прочего, сбор и/или проведение аудитов и обзоров безопасности, которые оценивают общее состояние безопасности в организации, и отчетность не реже одного раза в год перед исполнительным руководством для проверки и гарантии того, что уровень толерантности Поставщика к киберрискам не был нарушен.
3. Обеспечивать соблюдение Стандартов безопасности данных PCI (PCI-DSS), применимых к Поставщику, если Поставщик обрабатывает, хранит и/или передает транзакции, платежи и/или информацию по кредитным/дебетовым картам.
4. Поддерживать план управления кризисными ситуациями и план действий, а также план Группы реагирования на инциденты безопасности (SIRT) в соответствии с отраслевыми стандартами, чтобы гарантировать, что у Поставщика будут достаточные и адекватные возможности для обнаружения, сдерживания, расследования, реагирования и восстановления после любых попыток, подозрений и/или фактических инцидентов кибербезопасности.

17.63 Безопасность приложений, API, кода, системы и инфраструктуры

Если Поставщик осуществляет хостинг, разработку, совместную разработку, предоставление сред разработки и (или) поставку (а) программных приложений, Поставщик должен проводить проверку кода указанного программного обеспечения и (или) исправлений программного обеспечения для выявления недостатков безопасности и предотвращения несанкционированного доступа, модификации и (или) вставки вредоносного программного обеспечения или других форм вредоносного кода, а также тестирование на наличие уязвимостей, чтобы гарантировать, что приложение (включая API), наряду с базовыми системными службами, операционными системами и сетями, не содержит известных уязвимостей и дефектов, которые могут привести к инцидентам в сфере безопасности, нарушению конфиденциальности, мошенничеству, несанкционированному доступу и (или) разглашению Конфиденциальной информации, потере целостности обрабатываемой, хранящейся или передаваемой приложениями информации и (или) потере готовности, что может повлиять на качество продуктов и (или) услуг, которые Поставщик предоставляет Citi.

17.64 Мобильная безопасность

Если поставщик предоставляет мобильное приложение, Поставщик должен соответствовать следующим требованиям:

1. Мобильное приложение должно поддерживать только общедоступную (GA), устойчивую и не относящуюся к EOL² версию Google Android (кроме Android Go) и (или) платформы Apple iOS и iPadOS. Если мобильное решение оснащено поддержкой дополнительных операционных систем, поддерживаемые операционные системы (их версии) должны быть настроены компанией Citi.
2. Мобильное решение не должно поддерживать мобильные платформы / устройства, не оснащенные регулярными наборами инструкций для поддержки криптографических алгоритмов, включая, помимо прочего, шифрование, указанное в разделе 17.9 («Требования к шифрованию») настоящего документа.
3. Предварительные версии операционной системы, включая, помимо прочего, бета-версии, ознакомительные версии и версии, представляющие функции, не допускается использовать в производственной среде.
4. Поставщик должен быть в состоянии предоставить список интегрированных сторонних компонентов, включая, помимо прочего, бесплатные и открытые библиотеки программного обеспечения, которые объединяются/учитываются мобильным решением.
5. Мобильное приложение должно соответствовать требованиям и передовым методам, позволяющим публиковать мобильные приложения через открытые магазины приложений, например, Apple App Store или Google Play Store. Указанные открытые магазины приложений должны быть предпочтительным и основным методом распространения и размещения мобильного приложения.
6. Мобильные приложения Android должны использовать схему подписи APK v2+. Не допускается использование версии 1 Подписи APK (также известной как подпись JAR).
7. Тип и длина ключа подписи мобильного приложения должны соответствовать разделу 17.9 — Требования в отношении **шифрования** настоящего документа.
8. Каждый ключ подписи приложения и связанный с ним сертификат X.509v3 должны управляться индивидуально и предназначаться для одного ID приложения / ID связи. Ключ подписи не должен использоваться несколькими приложениями.
9. Если мобильное приложение требует сохранения данных на мобильном устройстве, оно должно сохранять только самые последние данные на

² Версии продуктов, которые активно поддерживаются и получают регулярные обновления безопасности и технического обслуживания от владельца платформы или Поставщика.

устройстве, необходимые для цели (целей) приложения/услуги или в течение того периода, пока это потребуется в соответствии с законодательными или нормативными требованиями.

- a. Сбор, обработка и/или хранение пользовательских данных должны соответствовать местным законам, включая, помимо прочего, такие правила конфиденциальности, как Общий регламент по защите данных (GDPR) и Директива 2002/58/ЕС (ePrivacy) или их региональные эквиваленты.
- b. Интегрированные сторонние компоненты (например, библиотеки) не должны осуществлять сбор, обработку и/или хранение пользовательских данных.

10. Мобильные приложения не должны предоставлять доступа к миру данных приложений.

- a. Если требуется обмен данными с другими приложениями, приложения должны использовать коммерчески обоснованные способы, методы и средства контроля для того, чтобы соответствующие операционные системы передавали только необходимый объем данных минимальному числу других приложений в тех случаях, когда такой обмен данными является надлежащим образом обоснованным и задокументированным.

11. Мобильные приложения должны полагаться исключительно на безопасные средства связи, предоставляемые соответствующими мобильными операционными системами. Например:

- a. Приложения Android должны прямо указывать на то, что незащищенный сетевой трафик не разрешен в любом сетевом домене, в манифесте приложения и/или в файле конфигурации сети.
- b. Приложения iOS/iPadOS должны использовать Application Transport Security (ATS) без каких-либо исключений.

12. Криптографические материалы должны быть привязаны к защищенному хранилищу ключей с аппаратной поддержкой.

13. Мобильные приложения должны быть созданы в режиме релиза и не должны содержать:

- a. Любых функций или методов, способных обойти контроль безопасности,
- b. Информации об отладке, например, имена файлов исходного кода, имена переменных, имена символов, комментарии и т. д., которая может облегчить обратное конструирование.

14. Мобильные приложения должны быть оснащены эффективными механизмами защиты от подслушивания или подмены, чтобы

предотвратить внедрение вредоносного кода, который может изменять или контролировать поведение приложения во время работы.

15. В мобильных приложениях должны быть реализованы комплексные методы защиты от отладки или обратного конструирования / обфускации для предотвращения атак обратного конструирования.
16. Пакеты мобильных приложений должны быть оснащены возможностью проверки подлинности и целостности их содержания (например, с использованием криптографической контрольной суммы и/или цифровой подписи).
17. Если мобильное приложение требует аутентификации пользователя, проверки целостности приложения и/или устройства должны быть выполнены до начала аутентификации пользователя.
18. Мобильные приложения, которые получают доступ к информации, находящейся в собственности Citi и классифицированной Citi как конфиденциальная информация или информация более высокого уровня защиты, обрабатывают такую информацию или хранят ее и (или) если классификация риска ИБ таких приложений для этой информации имеет значение «Средний» или выше, должны использовать только сильные биометрические модальности (например, они должны соответствовать категории Class 3 / Strong или превосходить ее, как определено в соответствующем документе [Android Compatibility Definition Document](#)).
19. Мобильные приложения должны применять контрмеры для защиты от атак типа «человек посередине» (Man-in-the-middle, MitM).
20. Мобильные приложения должны уметь обнаруживать скомпрометированные устройства, включающие в себя, помимо прочего, «разлоченные» или «рутованные» мобильные устройства, и реагировать на них в соответствии с оценкой рисков компании и регуляторными требованиями.
21. Мобильные приложения должны обеспечивать надежную привязку к устройству, чтобы предотвратить клонирование программного маркера (например, доказательства владения).
22. Мобильные приложения должны использовать безопасные клавиатурные приложения / решения (например, встроенные / предварительно установленные мобильными операционными системами).
23. Push-уведомления не должны содержать никакой конфиденциальной информации (например, информации Citi, классифицируемой как конфиденциальная или более высокого уровня защиты). Тем не менее, одноразовый пароль (OTP) может распространяться через push-уведомление.
24. Решения для мобильных приложений должны быть оснащены возможностью отклонений/игнорирования попыток связи с мобильными клиентами, использующими версию(и) приложения с известными/исследуемыми уязвимостями.

25. Мобильные приложения должны придерживаться передовых отраслевых практик, включая, помимо прочего, методы предотвращения, опубликованные в [OWASP Mobile Top 10](#).
26. Мобильные приложения, использующие методы искусственного интеллекта и машинного обучения (AI/ML), должны использовать такие методы этично и в соответствии с разделом 19 — **Error! Reference source not found.** (включая «Генеративный искусственный интеллект и агентный искусственный интеллект»).
27. Мобильное приложение должно использовать минимальные разрешения для устройства, необходимые для выполнения цели (целей) / функции, которые используются Citi.
28. Мобильные приложения не должны хранить никакой закрытой информации на внешнем/съёмном носителе, например, на SD-карте.**Error! Reference source not found.****Error! Reference source not found.**

17.65 Разглашение информации о программном обеспечении

Поставщик обязан разглашать информацию обо всех без исключения компонентах программного обеспечения, включая, помимо прочего, программное обеспечение с открытым исходным кодом, содержащееся в любых продуктах и услугах, предоставляемых Citi (совместно именуется «Компоненты программного обеспечения»). Поставщик обязуется не включать никакие компоненты программного обеспечения в любую версию Продуктов или Услуг, которые должны быть установлены в системах Citi, посредством обновления, модернизации или иным образом, не предоставив предварительно соответствующую информацию компании Citi в каждом случае. Кроме того, Поставщик должен обеспечить, чтобы его продукты и услуги не включали в себя компоненты программного обеспечения, лицензированные на условиях, в соответствии с которыми компания Citi или ее Аффилированные лица должны нести обязательства, которые не были прямо разглашены и приняты компанией Citi в Соглашении. Поставщик обязуется сообщать Citi о любых вредоносных Компонентах программного обеспечения, обнаруженных в организации, продуктах или услугах Поставщика, в течение 30 дней с момента их обнаружения. В частности, Поставщик обязуется разглашать информацию об использовании компонентов программного обеспечения в каждом выпуске и каждой версии продуктов или услуг посредством предоставления компании Citi спецификации программного обеспечения (SBOM) в формате файла OWASP CycloneDX или в формате файла спецификации ISO/IEC 5962:2021 Software Package Data Exchange (SPDX). В рамках такого разглашения следует указать источник происхождения программного обеспечения (например, коммерческий поставщик, встроенная база данных, общедоступный диспетчер бинарных пакетов, создано из исходного кода, поставщик встроенного программного обеспечения или рекомендованный поставщик компонентов программного обеспечения), взял ли поставщик или любая из подчиненных ему сторон копию компонентов программного обеспечения (которую называют «вилка») и включил ли ее впоследствии в свой продукт или услуги в качестве зависимости

пакетов или исходного кода, интегрированного в исходный код Поставщика, на основе которого были скомпилированы продукты и услуги.

17.66 Моделирование угроз

Поставщик должен внедрить процесс моделирования угроз, который всесторонне учитывает и (или) включает в себя все следующие компоненты.

1. Определение области действия. Поставщик должен четко определить область действия модели угроз, уделив основное внимание компонентам программного обеспечения и потокам данных, которые обрабатывают, хранят или передают конфиденциальную информацию Citi и более секретную информацию.
2. Выявление угроз. Поставщик должен систематически выявлять потенциальные угрозы и уязвимости, связанные с дизайном, архитектурой и предполагаемым использованием программного обеспечения, с учетом различных векторов атак и участников угроз на ранних этапах жизненного цикла разработки программного обеспечения.
3. Анализ рисков. Поставщик должен анализировать выявленные угрозы, чтобы оценить их потенциальное воздействие и вероятность их возникновения, что позволит определить приоритетность рисков безопасности.
4. Интеграция средств контроля. Поставщик должен определить и интегрировать соответствующие средства контроля безопасности и стратегии уменьшения рисков в разработку и проектирование программного обеспечения для устранения этих приоритетных рисков.
5. Документация. Поставщик должен документально зафиксировать модель угроз, в том числе выявленные угрозы, связанные с ними риски и соответствующие принятые меры по их уменьшению.
6. Периодическая проверка. Поставщик должен регулярно проверять и обновлять модели угроз, в частности, при существенных изменениях в проекте, функциональных возможностях и среде развертывания программного обеспечения.

17.67 Искусственный интеллект

1. Поставщики должны внедрить и соблюдать надежный жизненный цикл разработки защищенного программного обеспечения (SSDLC) для всех систем и компонентов искусственного интеллекта и машинного обучения, предоставляемых компании Citi или интегрированных в ее деятельность. Это требование включает в себя безопасное проектирование, разработку, тестирование, развертывание и непрерывное обслуживание.
2. Предоставляемые поставщиком системы искусственного интеллекта должны обеспечивать целостность операций и хорошо отлаженное сопротивление злонамеренным атакам. Это требование включает в себя внедрение механизмов быстрого обнаружения атак с использованием внедрения инструкций, «санитарной» обработки входных данных и обеспечения изоляции данных.

3. Агенты и компоненты искусственного интеллекта, предоставляемые поставщиками, должны безопасно взаимодействовать с системами Citi и другими инструментами. Для этого требуется эффективное управление идентификационной информацией и доступом, строгая проверка аргументов в отношении использования инструментов и изоляция операций инструментов с высоким риском. Механизмы Human-in-the-Loop (HITL) должны быть внедрены для выполнения действий, связанных с секретной информацией и высоким риском.
4. Системы искусственного интеллекта Поставщика должны создавать всеобъемлющие, не подлежащие изменению и подлежащие проверке журналы для всех значительных событий. Эти журналы должны быть защищены от подделки, а также их следует объединять в одно целое и хранить в соответствии с политиками Citi. Для выявления инцидентов и подозрительных действий в сфере безопасности и оповещения о них требуются возможности для непрерывного мониторинга и обнаружения отклонений.
5. Системы искусственного интеллекта Поставщика должны поддерживать надзор со стороны человека на основе оценки рисков, позволяющий принимать соответствующие меры. Такие системы должны быть разработаны с учетом четкой ответственности за результаты и действия искусственного интеллекта. Это требование включает в себя классификацию результатов искусственного интеллекта по уровням риска и поддержку возможностей замещения со стороны человека.
6. Все агенты, компоненты и системы искусственного интеллекта, предоставляемые поставщиками, должны внедрять надежные средства контроля за управлением идентификационными данными и доступом. Каждое взаимодействие с искусственным интеллектом должно быть связано с идентификационными данными, позволяющими установить личность (человека или неживого объекта), а для любого доступа требуется проверка подлинности. При доступе к ресурсам Citi агенты искусственного интеллекта должны использовать управляемые идентификационные данные и соблюдать принципы минимальных привилегий.
 - a. Поставщики должны обеспечить, чтобы всем агентам искусственного интеллекта были назначены идентификационные данные агентов Citi Object Identity Network (COIN) объединенные с системами Citi Identity and Access Management (IAM), чтобы обеспечить применение политик безопасности Citi, централизованное управление идентификационными данными и возможность проведения проверок.
 - b. Поставщики должны принять на обслуживание сторонних агентов в COIN, используя утвержденные Citi механизмы интеграции, включая COIN API, доступный через шлюзы системы безопасности (например, SSG Gateway или Arigee), а также они должны обеспечить, чтобы такой прием на обслуживание осуществлялся безопасным образом в соответствии с применимыми требованиями безопасности Citi.

- с. Поставщики, если их системы размещаются внутри компании, должны генерировать свой токен, который соответствует COIN. Поставщики, системы которых размещаются за пределами компании и осуществляют проверку подлинности входных запросов, используя свой собственный объединенный токен, должны поддерживать обмен токенов на токены Citi, например, обмен токенов MSFT на токены COIN. Любой новый тип токена, который в настоящее время не поддерживает обмен токенами, должен быть проверен сотрудниками IAM в Citi с целью определения возможности поддержки его обмена.
- 7. Если поставщики используют или предоставляют серверы или клиентов протокола Model Context Protocol (MCP), они должны внедрить MCP RFC 7591, включая все дополнительные функции.
- 8. Системы искусственного интеллекта Поставщика должны защищать системные подсказки и внутреннюю работу, чтобы не допустить разглашения информации о них и манипулирование ими. Управление контекстом должно обеспечить жесткие рамки для предотвращения утечки данных между арендаторами, пользователями и средами.
- 9. Поставщики должны документально зафиксировать процедуры обнаружения инцидентов безопасности искусственного интеллекта, реагирования на них и информирования о них, в том числе в отношении злонамеренных атак, манипулирования моделями, несанкционированных действий, связанных с искусственным интеллектом, или нарушения данных, связанного с системами искусственного интеллекта. Компания Citi должна быть немедленно уведомлена о любых таких инцидентах.

18 РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НА РАБОЧЕМ МЕСТЕ

Применимо к Поставщикам, которые получают доступ к информации Citi, обрабатывают такую информацию, хранят ее или управляют ею И (ИЛИ) осуществляют хостинг интернет-приложений под брендом Citi И (ИЛИ) имеют возможность подключения к сетевым ресурсам Citi И (ИЛИ) которым требуется доступ на объекты Citi без сопровождения.

Поставщики должны обеспечивать сохранность материальных и нематериальных активов Citi и ее клиентов. Активы Citi и активы клиентов можно использовать только в разрешенных целях и согласно установленному порядку (например, в соответствии с применимыми лицензиями, условиями и положениями) с учетом бизнес-целей Citi и ее поставщиков. Активы включают в себя наличные деньги, ценные бумаги, физическую собственность, услуги, бизнес-планы, информацию Citi, информацию о поставщиках, информацию о дистрибьюторе, интеллектуальную собственность (компьютерные программы, модели и другие предметы) и всю другую личную, внутреннюю и конфиденциальную информацию. Незаконное присвоение или несанкционированное раскрытие активов Citi является

нарушением ваших обязательств перед Citi и может стать причиной обвинения Citi в мошенничестве. Аналогичным образом халатное отношение, растрата, несанкционированное использование активов Citi является нарушением ваших обязательств перед Citi.

Элемент	Требования
Информация Citi (электронная и печатная документация)	По окончании рабочего дня, а также во время нахождения за пределами рабочего места Поставщик обязан блокировать доступ к информации Citi и принимать меры по ее защите.
Персональные компьютеры (ПК) и ноутбуки	ПК и ноутбуки, используемые для доступа или просмотра любой информации Citi, должны быть защищены паролями для сохранения экрана после периода бездействия. Когда Поставщик покидает рабочее пространство, он должен заблокировать ПК и/или ноутбук с помощью команды CTRL + ALT + DEL и выбрать «Lock Computer». Если Поставщик пользуется ноутбуком для просмотра информации Citi, в рабочее время ноутбук должен быть прикреплен к стационарному блоку посредством замка или троса безопасности, а в нерабочее время — закрыт на замок в надежном месте.
Запирание	В нерабочее время шкафы для документов и картотечные ящики, где хранится информация Citi, должны быть заперты на замок.
Открытые офисные зоны	Открытые офисные зоны не должны использоваться в качестве файловых серверов или мини-центров обработки данных для хранения информации Citi, за исключением случаев, когда они специально предназначены для такого использования и такое использование документально подтверждено Citi.
Принтеры, ксероксы и поддоны факсов	Запрещено оставлять материалы, имеющие отношение к Citi, в лотках принтеров, фотокопировальных аппаратов и факсов.
Уничтожение	Уничтожение информации Citi, которая больше не требуется (с указанием конкретных графиков хранения). Документы необходимо shredировать или помещать в изолированный / запираемый мусорный контейнер. Магнитные носители должны быть надежно уничтожены после соблюдения надлежащих процедур удаления.

19 ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ (ВКЛЮЧАЯ ГЕНЕРАТИВНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И АГЕНТНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ)

Применимо к Поставщикам, которые используют искусственный интеллект и машинное обучение (AI/ML), включая генеративный искусственный интеллект и агентный искусственный интеллект, в соответствии с определением Citi в настоящих Требованиях для Поставщиков, в любой части продукта или услуги, которые они предоставляют.

19.1 Поставщик не должен использовать искусственный интеллект и машинное обучение, описанные ниже, и он должен гарантировать, что все его субподрядчики не используют такие искусственный интеллект и машинное обучение, за исключением случаев, когда такое использование было согласовано между Сторонами в соответствующем графике или заказе на выполнение работ по договору:

- а.** Используется, содержится или иным образом включается в любой продукт или услугу, которые прямо или косвенно предоставляются Citi по Договору, или в любую часть такого продукта или услуги, включая любые сторонние продукты или услуги, содержащиеся или встроенные в них; или
2. Используется каким-либо образом при выполнении Поставщиком любого Договора, вне зависимости от того, будут ли использоваться, содержаться или иным образом включаться такие AI/ML в фактический продукт или услугу, предоставляемую Citi; или
3. Используется Поставщиком любым способом, который может подвергнуть Информацию Citi воздействию такого ИИ/МО, включая, помимо прочего, любой ИИ/МО, используемый Поставщиком в его некоммерческих бизнес-операциях (например, ведение деловой документации, усовершенствование процессов, исследования и разработка, соблюдение и внутренний аудит).

19.2 Несоблюдение Поставщиком этих обязательств считается существенным нарушением условий настоящего Соглашения.

19.3 По запросу регулятора в рамках любой проверки регуляторным органом или судебного расследования использования AI/ML в любой части продукта или услуги Поставщик должен оказать Citi содействие в предоставлении ответа на запрос регулятора, включая проведение и (или) организацию проведения проверок алгоритмов, необходимых для выявления реальных операций алгоритмов, составляющих модели AI/ML.

19.4 Также необходимо соблюдать следующие принципы.

Правомочность. AI/ML Поставщика должны соблюдать применимое законодательство.

Цель и соразмерность цели. Поставщик не должен объединять Контент или информацию Citi с данными Поставщика или данными третьих сторон. Поставщик не должен использовать Контент или информацию Citi для обучения AI/ML без письменного разрешения Citi. AI/ML Поставщика не имеют права использовать Контент или информацию Citi, за исключением случаев, когда это необходимо для предоставления Услуг.

20. ЖАЛОБЫ КЛИЕНТОВ

20.1 Жалоба — это устное или письменное сообщение, которое может быть получено в устном виде (при личной встрече или по телефону) или письменном виде (по почте или с помощью электронных средств связи, таких как электронная почта, чат, социальные сети и т. д.) и в котором выражается недовольство клиента, лица, не являющегося клиентом, потенциального клиента, заказчика Citi, потенциального заказчика или уполномоченного представителя клиента (совместно именуются «Клиент») политикой Citi, продуктом или услугой, предлагаемыми Citi или посредством Citi, сотрудником Citi, подрядчиком Citi, сторонним поставщиком услуг, действующим от имени Citi, или этими лицами совместно в любом сочетании.

20.2 Поставщики должны соблюдать политику Citi Customer Complaint Handling Policy, а также все применимые стандарты и процедуры Citi в отношении жалоб. В случае получения Поставщиком любого письменного или устного сообщения о неудовлетворенности или проблеме (каждое из которых именуется «Жалоба») от любого Клиента (или лица, не являющегося Клиентом, или потенциального Клиента в соответствии с определением термина «Жалоба», принятым в Citi) или от любого Регуляторного органа в связи с Услугами, предоставляемыми Поставщиком от имени Citi, или по иной причине в связи с деятельностью Citi, Поставщик должен уведомить об этом основное контактное лицо бизнес-структуры Citi (или уполномоченное лицо) в письменной форме в течение двадцати четырех (24) часов с момента получения такого сообщения. Если Citi не предоставит такую систему Поставщику, Поставщик также должен разработать, внедрить и обслуживать систему отслеживания Жалоб («Система отслеживания»), которая будет обоснованно приемлемой для Citi, и предоставлять Citi по своему усмотрению копии отчетов или доступ к системе. Система отслеживания должна:

- a. классифицировать Жалобы по типу, дате получения и дате подачи уведомления о Жалобе в Citi;
- b. отслеживать ход рассмотрения Жалобы до вынесения заключения о ней или ее разрешения;
- c. предоставлять информацию по всем другим вопросам, которая может быть обоснованно затребована Citi. Система отслеживания должна быть разработана таким образом, чтобы позволить Поставщику определить, получает ли он чрезмерное количество Жалоб по конкретному вопросу, чтобы Поставщик (по согласованию с Citi) мог определить наличие системной проблемы, связанной с деятельностью Поставщика или предоставлением им Услуг, и незамедлительно исправить данные проблемы.

21. ПОЛИТИКА В ОТНОШЕНИИ ЛИЧНОЙ ТОРГОВЛИ И ИНВЕСТИЦИЙ

Политика Citi в отношении личной торговли и инвестиций (PTIP) определяет разрешенные и запрещенные торговые и инвестиционные операции, требования к предварительному утверждению, а также требования, касающиеся обслуживания, разглашения информации и надзора за брокерскими или торговыми счетами лица, на которое распространяется действие Политики. В этой политике установлены минимальные стандарты для обеспечения соблюдения законов и нормативно-правовых требований с целью предотвращения неправомерного использования должности лица или его взаимоотношений с Citi, включая знания этого лица о (1) существенной информации для служебного пользования или внутренней информации (совместно именуемой «Информация MNPI») в отношении Citi или третьей стороны; или (2) информации о ценных бумагах, деривативах, позиционировании товаров, транзакциях и стратегиях клиента.

Все сотрудники Поставщика, которым требуется регулярный доступ к Информации MNPI в рамках своих должностных обязанностей в Citi и которые назначены лицами, на которых распространяется действие Политики, и (или) лицами, имеющими доступ к информации Citi, должны соблюдать требования политики PTIP. Сотрудники поставщика должны соблюдать запросы ICRM, связанные с разглашением информации о личном счете, предварительным разрешением на личную торговую деятельность, ограничениями в отношении личной торговли и подачей периодических выписок по счету.

22. СТАНДАРТЫ ВЫСТАВЛЕНИЯ СЧЕТОВ

В рамках деятельности Citi по ускорению предоставления услуг и усовершенствованию средств контроля все Поставщики должны поддерживать предпочитаемые Citi методы предоставления счетов на оплату, а также предпочтительные варианты оплаты счетов, как описано ниже.

- Поставщик создает электронные файлы для передачи в Citi в формате, рекомендуемом Citi Поставщику, и (или) использует инструмент Citi iSupplier для ввода необходимых данных о счетах на оплату с целью их последующей цифровой передачи в Citi.
- Поставщик предоставляет Citi всю необходимую банковскую информацию и подтверждающую документацию для содействия электронным платежам Поставщику и (или) использует предложение Citi о виртуальных картах (в случае их наличия).

Примечание: условия оплаты рассчитываются, начиная с даты получения Citi счета на оплату.

Чтобы своевременно оплачивать счета и выполнять договорные обязательства, Citi требует от всех Поставщиков включать следующие данные в счета на оплату и соблюдать соответствующие инструкции после выставления Citi счетов за товары и услуги:

1. Надлежащая бизнес-структура Citi, адрес плательщика и имя соответствующего контактного лица в Citi.
2. Номер счета, дата выставления счета и номер заказа на покупку.
3. Счета на оплату должны быть отправлены на адрес или электронную почту Citi, указанные в заказе на покупку Citi.
4. Товары и услуги, за предоставление которых выставляется счет, должны быть точно указаны в счете с использованием пояснительной информации.
5. Только текущая сумма за конкретный счет (без учета других невыплаченных остатков по счетам).
6. Счета на оплату должны выставляться на английском языке, и подтверждающая документация должна быть предоставлена на английском языке.

23. ПОЛИТИКА ОБЯЗАТЕЛЬНОГО ОТСУТСТВИЯ НА РАБОЧЕМ МЕСТЕ

В соответствии с политикой компании Citi в отношении обязательного отсутствия требуется, чтобы лица, осуществляющие деятельность с использованием секретных данных или связанную с высоким риском, особенно деятельность, затрагивающую учетную документацию компании, периодически приостанавливали выполнение этих обязанностей. Такое принудительное отстранение от выполнения обязанностей предназначено для того, чтобы укрепить внутренние средства контроля путем создания возможностей для выявления возможного мошенничества, кражи или других неправомерных действий, которые в ином случае могут остаться невыявленными. Такая политика соответствует требованиям в отношении надзора, установленным Советом Федеральной резервной системы США в отношении, касающимся обязательного отсутствия на рабочем месте персонала, занимающего особо ответственные должности.

Все сотрудники Поставщика, которым требуется доступ к секретным данным в рамках своих должностных обязанностей в Citi и которые назначены лицами «занимающими особо ответственные должности», должны соблюдать требования политики МА. Лица, занимающие особо ответственные должности, обязаны ежегодно планировать и осуществлять в полном объеме обязательное отсутствие на рабочем месте в соответствии со всеми правилами и ограничениями политики. В течение этого периода они не должны осуществлять никакую особо ответственную деятельность, давать команды о ее проведении, уполномочивать других лиц на ее проведение и утверждать ее проведение, а также они не должны отвечать по существу на коммуникации, в том числе они не должны взаимодействовать с клиентами, за исключением случаев, когда они

переадресовывают запросы для рассмотрения другими сотрудниками. Если период обязательного отсутствия на рабочем месте должен быть прерван, когда он начался, руководители или контактные лица бизнес-структуры Citi должны аннулировать данный период обязательного отсутствия на рабочем месте в системах комплаенса, чтобы восстановить доступ к системе, после чего работник должен запланировать новый период обязательного отсутствия на рабочем месте.

ПРИЛОЖЕНИЕ — ОПРЕДЕЛЕНИЯ

Air – Gap — это мера безопасности, в рамках которой компьютер, система или сеть физически отделены от других компьютеров, систем и сетей. Архитектура резервного копирования данных при использовании технологии Air – Gap ограничивает подверженность сети кибератакам и позволяет восстановить данные по состоянию на определенный момент времени до начала атаки.

Применимое законодательство включает в себя: (а) законы и постановления штатов о лишении права выкупа и (b) правила, руководства и другие документы, выпущенные различными федеральными агентствами США, включая Управление финансового контролера (иногда называемые Руководящими принципами и положениями о тревожных признаках), реализующими раздел 114 Закона о добросовестном и точном проведении кредитных операций от 2003 г.

Зона доступности — это место, где Поставщик облачных услуг имеет группу центров обработки логических данных. Зона доступности — это один или несколько отдельных центров обработки данных с резервным питанием, сетью и телекоммуникациями в облачном регионе.

Искусственный интеллект (ИИ) — это количественный метод, система или подход («методы»), которые имитируют человеческий интеллект с помощью компьютерных программ для предоставления оценок, прогнозов, рекомендаций или решений способами, выходящими за рамки классических статистических, математических, эконометрических и финансовых подходов. Включает в себя все категории искусственного интеллекта, описанные ниже, а также разновидности искусственного интеллекта, например: модели генеративного искусственного интеллекта, модели агентного искусственного интеллекта, большие языковые модели, модели искусственного интеллекта общего назначения (GPAI) и т. д.

Категории ИИ включают в себя:

- о **Статический ИИ.** Методы искусственного интеллекта, тренируемые вручную в автономном режиме или имеющие параметры, которые явно запрограммированы, а затем используются для предоставления оценок, прогнозов, рекомендаций или решений.

- o **Динамический ИИ.** Методы, которые, в отличие от «статического ИИ», могут периодически автоматически переобучать параметры в ходе производственного процесса.
- o **Автоматический ИИ.** Методы «динамического ИИ», которые дополнительно способны автоматически изменять свою базовую структуру (например, гиперпараметры, входные переменные).
- o **Когнитивный ИИ.** Методы, которые могут автономно принимать решения и предпринимать соответствующие действия, даже по вопросам, для решения которых они не были специально обучены.

Машинное обучение (ML) — это подмножество искусственного интеллекта, которое извлекает представления или выводы из данных, не прибегая к явному программированию каждого представления параметра или шага компьютера, например, используя подходы на основе случайных лесов или нейронных сетей. Напротив, методы ИИ, которые не являются членами подмножества ML, включают такие методы, как нечеткая логика, сложные методы синтаксического анализа зависимостей для обработки естественного языка.

Специалист, отвечающий за деятельность подразделения (BAO) — это сотрудник Citi, ответственный за осуществление определенных видов деятельности, связанных со взаимоотношениями с поставщиками, и активное управление такими видами деятельности.

Коммерческий инициатор — это поставщик, привлеченный Citi к действиям от имени Citi для выявления новых коммерческих возможностей или управления существующими взаимоотношениями с клиентами.

Деловой подарок — любая ценная вещь (кроме корпоративных развлекательных мероприятий), предоставляемая сотруднику Citi или получаемая им в связи с деятельностью Citi или сторонней компании и, как правило, имеющая стоимость более 25 долларов США.

Информация Citi — это информация, которой Citi владеет или которую она обязуется защищать при хранении, обработке, передаче или утилизации в цифровом и нецифровом формате.

Информация Citi включает в себя следующие категории:

Конфиденциальная информация о бизнес-структурах Citi и/или связанных лицах, не относящаяся к физическим лицам и требующая высокого уровня защиты. Нарушение конфиденциальности, целостности или доступности данной информации может оказать серьезное влияние на операции, финансовое положение, франшизу или корпоративных клиентов Citi.

Конфиденциальная информация, позволяющая установить личность, — это Персональные данные лица, которые могут способствовать незаконной деятельности, а именно краже персональных данных, кредитному мошенничеству или другому финансовому мошенничеству в отношении данного лица. Нарушение конфиденциальности, целостности или доступности этой информации может оказать существенное влияние на физическое лицо (лиц), включая, помимо прочего, финансовые убытки или мошенничество.

- o Элементы персональных данных, которые в сочетании с другими личными данными представляют собой конфиденциальную PII, включают в себя имя лица или контактную информацию (адрес, телефон или адрес электронной почты) в сочетании со следующим:

- Элементы данных о транзакциях, которые могут привести к переводу средств или могут использоваться для хищения или мошенничества персональных данных, в том числе:
 - Номер кредитной/дебетовой карты
 - Код проверки подлинности карты (CVV) или PIN-код
 - Данные кредитного отчета (кредитный рейтинг)
 - Полная дата рождения
 - Трудовая деятельность (оценка/отзыв) или информация о компенсации
 - Видеозаписи, включая записи камер видеонаблюдения и банкоматов
- Отдельные элементы персональных данных должны представлять собой конфиденциальную информацию PII:
 - о Номер социального страхования США или идентификационный номер, выданный правительством (эквивалентный по статусу использования и/или правовой защиты номеру социального страхования США), номер паспорта, водительского удостоверения или индивидуальный номер налогоплательщика

Внутренняя информация — это информация не о физическом лице, которая предназначена для коммерческих целей и которой требуется умеренный уровень защиты. Нарушение конфиденциальности, целостности или доступности данной информации может оказать **ограниченное влияние** на группу или рабочую группу.

о **Информация, позволяющая установить личность (PII)**, — это любая информация, которая:

- Идентифицирует или может использоваться для идентификации человека или домохозяйства (например, имя, подпись, адрес, уникальный национальный идентификатор, например, номер социального страхования, регистрационный номер резидента, дата рождения, номер водительских прав).
- Относится, описывает, может быть соотнесена или может быть разумно связана (прямо или косвенно) с отдельным человеком или домохозяйством.
- Может использоваться для аутентификации человека или предоставления доступа к учетной записи (например, имя пользователя, адрес электронной почты, пароль, PIN-код, идентификационный номер, ответы на контрольные вопросы); или относится к физическому лицу и может носить конфиденциальный характер (например, личная медицинская информация или информация о здоровье, номер счета, сумма средств на счете).
- Персональная информация также включает защищенную медицинскую информацию (согласно определению Закона о преемственности и подотчетности медицинского страхования США), конфиденциальную личную информацию и кредитную информацию (согласно определениям различных законов о защите / конфиденциальности данных и конфиденциальности банков).

Публичная информация — это информация, которая находится в открытом доступе за пределами Citi или предназначена для широкой общественности, например, пресс-релизы и новостные статьи, посвященные Citi.

Информация с ограниченным доступом — это информация, которая используется определенными лицами или группами и которая является особо секретной для Citi или ее аффилированных лиц и требует самого высокого уровня защиты. Нарушение конфиденциальности, целостности или доступности этой информации может оказать **серьезное (в масштабах всей компании, нескольких регионов, нескольких секторов) влияние** на операции Citi, финансовое положение, франшизу или корпоративных клиентов.

- о **Секретная информация, которая позволяет установить личность (PII)** — это информация, которой в соответствии с определенными законами требуется дополнительная защита и которая может использоваться для незаконной дискриминации, иного проявления несправедливости или причинения вреда физическому лицу. Нарушение конфиденциальности, целостности или доступности этой информации может оказать существенное влияние на физическое лицо (включая, помимо прочего, финансовые убытки, мошенничество или дискриминационные последствия).
- Данные, которые непосредственно относятся к следующим признакам: раса, религия, религиозные или философские взгляды, этническое происхождение, политические взгляды или мнения, членство в профсоюзе, информация о наличии судимостей или уголовных преступлениях, генетические данные, биометрические данные или данные, касающиеся сексуальной ориентации или сексуальной активности человека.
- о Персональная информация о здоровье (PHI), которая включает в себя информацию о медицинской истории или психическом или физическом состоянии физического лица.

Клиент — любой клиент или заказчик Citi, в роли которого может выступать физическое или юридическое лицо, учреждение или организация.

Облачный регион — это физическое место, в котором Поставщик облачных услуг объединяет центры обработки данных.

Коммуникационное оборудование, системы и услуги — это любое оборудование, программное обеспечение или приложения, используемые для передачи письменных, голосовых или видеосообщений в электронном виде, в том числе (помимо прочего): компьютеры, ноутбуки, планшеты, мобильные устройства или мобильные телефоны, в том числе Bring Your Own Device (BYOD), BlackBerry, телефон, факсимильная связь (служба факсов), внутренняя сеть и доступ в Интернет, услуги Wi-Fi, услуги электронной почты, службы обмена мгновенными сообщениями, в частности, сообщениями в службах Microsoft Lync, Skype и Bloomberg, веб-сайты и приложения со встроенными функциями связи, платформы для видеоконференций или совместной работы, такие как Zoom и Microsoft Teams, а также службы социальных сетей, интерактивные службы обмена информацией, сторонние чаты, электронные доски объявлений и блоги.

Контент означает Конфиденциальную информацию Citi и любые другие данные, отчеты, статистические данные или информацию любого рода (а) предоставленные или переданные Поставщику Citi или ее Аффилированными лицами или от их имени, или от имени и по поручению их клиентов, подрядчиков или поставщиков услуг, (б) созданные,

произведенные с помощью Услуг, или (в) полученные в результате любого из вышеперечисленного.

Договор — письменный юридический документ, подписываемый двумя или более сторонами и содержащий предложение, подписи, основание сделки, обязательства сторон и правовое обоснование. Примеры договоров могут включать в себя генеральные соглашения в отношении продуктов и услуг, техническое задание и заказ на выполнение работ, поправки и дополнения, планы работ, заказы или иные письменные документы, подписываемые организацией, входящей в состав Citi, и поставщиком. В целях настоящих Стандартов соглашение о неразглашении конфиденциальной информации (NDA) также считается договором.

Испытание на отказ в предоставлении доступа (DOA) оценивает комплектность персонала Поставщика и поддержку для бизнес-процессов Citi, которые могут быть восстановлены в рамках установленного целевого времени восстановления (RTO).

Испытание на отказ в обслуживании (DOS) подтверждает, что приложение Поставщика и базовые компоненты инфраструктуры, поддерживающие бизнес-структуру Citi, могут быть восстановлены в рамках установленного целевого времени восстановления (RTO).

Материалы, подлежащие сдаче на хранение — означает следующие подразделы (i)-(vi) в совокупности в отношении (в соответствующих случаях) программного обеспечения, лицензия на которое предоставляется Citi для работы в среде Citi, или материалов, используемых Поставщиком для размещенных услуг, предоставляемых Citi:

- (i) Точная дублированная версия исходного кода для программного обеспечения, используемого для разработки, эксплуатации, обслуживания и поддержки лицензированного программного обеспечения или размещенных услуг, определенных в применимом соглашении с Citi (и всех последующих версий такого программного обеспечения или размещенных услуг), а также вся документация по такому программному обеспечению (независимо от того, может ли Citi уже иметь копию частей такого исходного кода) («Сдача на хранение исходного кода»).
- (ii) Исходный код любого стороннего программного обеспечения, на которое Поставщик имеет права в отношении разработки, эксплуатации, обслуживания и поддержки лицензированного программного обеспечения или размещенных услуг.
- (iii) Лицензированная копия всех программных инструментов, таких как отладчики, сборщики и компиляторы, необходимых для преобразования исходного кода, включенного в материалы, подлежащие сдаче на хранение, в исполняемую форму в случае необходимости для работы, обслуживания и поддержки программного обеспечения или размещенных услуг.
- (iv) Если не было определено выше, любая документация, предоставляющая следующую информацию: (A) общее описание и функционирование материалов, подлежащих сдаче на хранение, (B) архитектура и основные программные функции; (C) информация о потоках данных; (D) подробная карта памяти и перечень распределения памяти; (E) карты портов ввода и вывода; и (F) другие данные, которые позволили бы программисту, обладающему обычным опытом в соответствующем языке (языках) программирования, использовать и изменять исходный код, включенный в материалы, подлежащие сдаче на хранение.
- (v) Любая другая техническая информация, связанная с программным обеспечением или размещенными услугами, которая обоснованно требуется, чтобы позволить Citi или компетентному третьему лицу от имени Citi использовать, эксплуатировать,

модифицировать и совершенствовать программное обеспечение или размещенные услуги.

- (vi) Список всех сторонних программ и технологий, используемых в связи с программным обеспечением или размещенными услугами, включая обоснованную информацию о его использовании в программном обеспечении и контактную информацию для поставщика такого программного обеспечения или технологии. Citi признает и соглашается, что материалы, подлежащие сдаче на хранение, не содержат никаких исходных кодов третьих лиц, кроме указанных в подразделе (ii);

и

- (vii) В отношении размещенных услуг:

- a. уменьшенная копия облачной производственной среды или материалы, относящиеся к облачной среде определенной среды, и другая информация, необходимая для воспроизведения производственной среды Citi, включая (помимо прочего) инфраструктуру, такую как код, сценарии terraform, облачный ресурс, шаблоны формирования облачной среды, файлы конфигурации, арендаторов облачной среды, подписки на облачные сервисы, изображения моделей, изображения пристыкованных программ и инфраструктуру как исходный код Программного обеспечения; и
- b. копия данных Citi, хранящихся в Программном обеспечении.

Электронные коммуникации — это сообщения или данные, отправляемые, получаемые или используемые Персоналом с использованием электронных средств, передаваемые по проводам или с помощью беспроводных сигналов. Электронные коммуникации включают в себя, помимо прочего, текстовые сообщения, электронную почту, одноранговые или мгновенные сообщения, публикации в блогах, сообщения в социальных сетях, сообщения, отправленные через приложения для обмена сообщениями, такие как WhatsApp, WeChat, Line, Signal или Viber, а также вложения, снимки экрана, записанные голосовые файлы или видеофайлы и файлы, аудио- или видеотрансляцию в режиме реального времени, и файлы, созданные, полученные, загруженные, сохраненные, переданные, удаленные или используемые через оборудование, системы и сервисы электронной коммуникации.

Функциональные идентификаторы — это общие идентификаторы, такие как ADMIN или ROOT, используемые лицом или процессом для получения доступа к системе безопасности. Ключевой инициативой в рамках управления идентификацией и доступом (IAM) является обеспечение наличия у Citi конкретных, четко определенных способов контроля для защиты от рисков, сопряженных с использованием функциональных идентификаторов.

Критичные для франшизы процессы и критичные для франшизы приложения (FCA) — это процессы и приложения, которые Citi определяет как имеющие важнейшее значение для осуществления критически важных коммерческих функций в рамках франшизы.

Мошенничество — это умышленное действие, введение в заблуждение или бездействие с целью обмана других лиц, в результате чего жертва несет убытки или преступник получает выгоду.

Размещенные услуги включают в себя любые установленные приложения, а также любые средства и среду, управляемые или используемые Поставщиком для предоставления размещенных услуг, все приложения и другое программное обеспечение, базы данных, веб-сайты, серверы, оборудование, сети, телекоммуникационное и другое оборудование, а также другие установленные или используемые технологии в среде размещенных услуг,

а также, в каждом случае, все обновления и услуги поддержки, за исключением всего контента и систем Citi.

Данные проверки идентификации (IVD) определяются как вопросы безопасности (SQ) или вопросы проверки подлинности на основе знаний (КВА). Вопросы безопасности, как правило, определяются приложением, а ответы на них дает конечный пользователь. Примерами являются девичья фамилия матери, место рождения, любимое мороженое и т.д. Оба типа вопросов должны рассматриваться как «Данные аутентификации».

Информационная безопасность или «ИБ» — состояние, в котором компьютер или компьютерная система защищены от несанкционированного доступа или атаки, и в этом состоянии (а) компьютер или компьютерная система продолжают быть доступными и работоспособными; (b) не нарушена целостность компьютера или компьютерной системы; и (c) сохраняется целостность и конфиденциальность информации, которая хранится в компьютере или компьютерной системе, обрабатывается компьютером или компьютерной системой или передается через компьютер или компьютерную систему.

Угроза ИБ означает действие или активность (известную или подозреваемую), осуществляемую на компьютере или в компьютерной системе или через нее, которая может поставить под угрозу или отрицательно повлиять на ИБ этого или другого компьютера или компьютерной системы.

Уязвимость ИБ означает любую уязвимость компьютера или компьютерной системы, которая может быть использована одним или несколькими угрозами ИБ.

Несвязанная с клиентами и негенерирующая доход деятельность определяется как критически важные для деятельности компании действия, несвязанные с генерированием дохода, включая юридическую, надзорную и регуляторную деятельность, а также деятельность по обеспечению непрерывности коммерческой деятельности.

Соглашение о разглашении информации (NDA) — это соглашение между Citi и Поставщиком, в соответствии с которым обмен, использование и раскрытие информации регулируются условиями договора.

Программное обеспечение с открытым исходным кодом означает исходный код или компилированную компьютерную программу, исходный код которой доступен широкой публике для использования или изменения изначального дизайна.

Персонал: означает, независимо от того, указано ли это непосредственно или понимается из контекста, Поставщика и его аффилированных лиц, директоров, должностных лиц, сотрудников, агентов, аудиторов, консультантов, поставщиков услуг и подрядчиков (кроме персонала Citi). В состав персонала Поставщика также входят директора, должностные лица, сотрудники, агенты, аудиторы, консультанты или другие представители любого субподрядчика.

Журнал документации — подробный перечень типов документов, местонахождения, дат и других сведений о документах Citi, необходимый компании для управления документооборотом на протяжении всего жизненного цикла информации.

Требование о хранении информации — это требование в отношении документов и информации, запрещающее вносить изменения в них или уничтожать их до момента отзыва этого требования организацией, которая его выдала.

Способность восстановления — объем, количество или скорость предоставления продуктов и услуг Поставщика в процентах от нормальных показателей предоставления продуктов и услуг.

Длительность восстановления — максимальный срок (в календарных днях), в течение которого Поставщик может осуществлять деятельность, находясь в режиме восстановления.

Целевая точка восстановления — точка на шкале времени в прошлом (в часах), до которой требуется восстановить данные после прерывания деятельности. Это максимальный целевой период, в течение которого данные могут быть утеряны службой ИТ вследствие крупного инцидента. ЦТВ — это лишь значение максимального периода времени, в течение которого данные могут быть утрачены, если имеет место серьезный инцидент, затрагивающий ИТ-сервис. Она не является прямым показателем того, сколько данных может быть потеряно, например, к концу обработки предыдущего дня.

Целевое время восстановления — период времени в часах между прерыванием и восстановлением обслуживания и предоставления продуктов и услуг.

Событие передачи материалов, подлежащих сдаче на хранение, означает одно или несколько из следующих действий.

- (i) Поставщик (А) становится неплатежеспособным или признает свою неспособность погасить долги в целом, когда наступает срок их погашения; (В) становится субъектом (добровольно или недобровольно) судебного разбирательства в соответствии с местным или иностранным законом о банкротстве или несостоятельности, которое не приостанавливается полностью в течение семи (7) рабочих дней и не прекращается и не отменяется в течение сорока пяти (45) дней после подачи иска; (С) осуществляет общую уступку прав в интересах кредиторов; или (D) имеет получателя, доверительного управляющего, распорядителя или аналогичного представителя, назначенного по распоряжению любого суда компетентной юрисдикции для принятия на себя ответственности за существенную часть имущества или компании Поставщика или продажи существенной части имущества или компании Поставщика.

Организация по управлению ресурсами (RMO) отвечает за глобальное комплексное управление ресурсами для Citi, включая стратегический выбор источников поставки ресурсов, операции «от закупки до платежа», подбор кадров и структуру управления поставщиками.

Менеджер по снабжению RMO — это участник Организации по управлению ресурсами (RMO), ответственный за обсуждение условий заключения договора, требований и цен, в том числе

за запрос предложений и прочие мероприятия по выбору поставщика, соблюдение условий и положений договора, финансовую оценку квалификационных требований.

Серьезные или катастрофические негативные последствия для физического лица означают, что воздействие может иметь значительные негативные последствия для данного человека, включая финансовый ущерб, потерю работы или потерю трудоспособности, потерю прав человека, личное или публичное унижение или неправомерное лишение свободы.

Субподрядчик — это четвертое лицо (физическое или юридическое лицо), нанятое третьим лицом для оказания некоторых или всех услуг или видов деятельности, по которым Citi заключила договор с третьим лицом.

Руководство:

В1. Нужно ли сообщать обо всех субподрядчиках третьего лица?

О1. Необходимо сообщать только о субподрядчиках, связанных с оказываемой услугой. К примерам услуг или деятельности, выполняемых субподрядчиком, относятся, помимо прочего:

*Субподрядчик, предоставляющий технологические или программные услуги, прямо или косвенно поддерживающие услугу/активность, с которыми Citi заключила договор с Третьим лицом; или

*Субподрядчик, услуги которого включают в себя доступ к конфиденциальной информации Citi или информации более высокого уровня защиты; или

*Субподрядчик, осуществляющий прямое или косвенное взаимодействие с любым существующим/потенциальным клиентом Citi; или

*Субподрядчик, не требующий эскалации и предоставляющий услуги по шредированию или архивированию документов Citi в рамках или за пределами любого помещения Citi; или

*Субподрядчик, поддерживающий основные банковские функции или услуги, такие как платежи, сбор, кредитование и т. д.

Поставщик. В целях настоящего документа «Требования Citi к поставщикам» «Поставщик» относится исключительно к внешнему третьему лицу, заключившему деловое соглашение о предоставлении продуктов или услуг непосредственно юридическому лицу Citi или о поддержке юридического лица Citi в рамках достижения его коммерческих целей. Внешнее третье лицо определяется как юридическое лицо, не входящее в состав Citi. Поставщики также могут быть клиентами или заказчиками юридического лица Citi или взаимодействовать с клиентами и заказчиками Citi, однако договоренности, основанные исключительно на том, что они являются клиентами или заказчиками Citi, не считаются отношениями с поставщиками в рамках настоящего документа.

Временные данные. Документ — это окончательная, наиболее полная версия информации, которую Citi обязана хранить по юридическим, нормативно-правовым или экономически обоснованным причинам. Все остальные данные классифицируются как временные данные.