Приложение № 1
к Приказу № 77-ОД
от «21» июля 2021 года

Стандарт информационной безопасности для подрядчиков

Стандарт информационной безопасности для подрядчиков (далее – Стандарт) устанавливает требования и рекомендации, предъявляемые СберРешениями[1] (далее - Компания) к третьим лицам/поставщикам/подрядчикам (далее каждый по отдельности — Подрядчик) и необходимые для обеспечения информационной безопасности и защиты интересов Компании при использовании Подрядчиками информационных активов Компании. Настоящий Стандарт применим ко всем Подрядчикам и их субподрядчикам, которые хранят, обрабатывают или имеют доступ к данным Компании. Требования настоящего Стандарта в обязательном порядке включаются в договоры с Подрядчиками, которые хранят, обрабатывают или имеют доступ к данным Компании.

Любые дополнительные обязательства Подрядчика в отношении информационной безопасности по любому соглашению с Компанией являются дополнением к требованиям, изложенным в настоящем Стандарте.

В контексте настоящего Стандарта термин «Информация» включает как Конфиденциальную информацию, так и Персональные данные, используемые в процессе осуществления коммерческой деятельности (далее по отдельности и (или) совместно именуемая — «Информация»). Персональные данные означают любую информацию, относящуюся прямо или косвенно к определенному или определяемому лицу (п. 1 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»). Конфиденциальная информация означает любую конфиденциальную или служебную информацию, определение которой приведено в NDA между Подрядчиком и Компанией.

Настоящим поясняется, что данный Стандарт применим ко всей Информации, обрабатываемой Подрядчиком, в том числе, обрабатываемой при:

- создании;
- редактировании;
- управлении;
- получении доступа;
- получении;
- передаче;
- уничтожении;
- хранении или размещении на сервере в любом формате, в том числе, среди прочего:
    - в системах;
    - в облачной среде;
    - в среде промышленной и непромышленной эксплуатации;
    - в ресурсах, находящихся в памяти ЭВМ и на электронных устройствах (включая предоставленные компанией устройства и устройства, используемые в соответствии с «концепцией использования сотрудниками личных устройств»);
    - версии такой Информации на неэлектронных носителях.

Компания оставляет за собой право проводить аудит Подрядчиков и их субподрядчиков, если они не предоставляют гарантий соответствия требованиям сертификации ISO/IEC 27001 или SSAE 18 (SOC2) на ежегодной основе. Для этого Компания предоставляет письменное уведомление, за исключением

[1]СберРешения - Группа компаний «Интеркомп» (АО «Интеркомп», ООО «Интеркомп Аутсорсинг», ООО ЧАЗ «Интеркомп», ООО ЧАЗ МК «Персонал», ООО «ЦБУ «Интеркомп», ООО «БУиК», ООО «СберРешения», ТОО «Интеркомп Казахстан», ТОО «Интеркомп аутсорсинг-Казахстан», ООО «Интеркомп аутсорсинг Азербайджан», ООО «Интеркомп Грузия»).

случаев, когда Компания имеет разумные основания подозревать мошенничество или серьезное нарушение требований обработки Информации подрядчиком, и в этом случае аудит может быть проведен в любое время с предварительным письменным уведомлением не менее чем за десять (10) рабочих дней.

Компания вправе приостановить доступ к Информации Компании работнику Подрядчика в случае нарушения им требований настоящего Стандарта.

Подрядчик должен разрешить Компании запрашивать и/или проводить за счет Компании не более двух оценок или аудитов безопасности в год, включая, но не ограничиваясь: обзор политик, процессов и процедур; оценку механизмов обеспечения информационной безопасности (физической безопасности и конфиденциальности Информации).

Критерии проведения аудита включают соблюдение Подрядчиком требований контроля и положений, определенных в стандартах ISO/IEC 27001 и SSAE 18 (SOC2) (если применимо), а также в настоящем Стандарте.

Требования информационной безопасности для подрядчиков

1. Правила и процедуры обеспечения информационной безопасности

Подрядчик должен принять и соблюдать задокументированные политики, стандарты и процедуры в отношении информационной безопасности в целях создания контролируемой среды (далее - Среда), связанной с защитой конфиденциальности, целостности и доступности информации. Политики и процедуры подлежат ежегодному пересмотру, обновлению и утверждению высшим руководством.

Если Подрядчик разрешает использование личных устройств для доступа к Информации или системам, то ему необходимо внедрить Политику «использования сотрудниками личных устройств» (концепция BYOD).

2. Руководство и обучение

Персонал Подрядчика должен пройти соответствующее обучение по утвержденной программе в области обеспечения информационной безопасности, включая требования к защите и безопасной работе с Информацией. Материалы программы обучения должны периодически пересматриваться и обновляться. По запросу необходимо предоставлять краткий обзор завершенного обучения.

При заключении договора Подрядчик обязуется определить своего представителя в качестве единственного контактного лица по всем вопросам, связанным с информационной безопасностью. В дополнение Подрядчик должен определить представителя, ответственного за контроль соблюдения настоящего Стандарта.

3. Правила обеспечения безопасности со стороны кадровых ресурсов

Подрядчик должен обеспечить подписание работниками Подрядчика до начала работ по договору обязательства о неразглашении сведений конфиденциального характера и соблюдения требований информационной безопасности и передать оригиналы этих обязательств Компании в течение 10 рабочих дней после подписания путем направления заказным письмом с уведомлением о вручении или передачи уполномоченному работнику Компании.

При получении от Компании информации о внесении изменений в настоящий Стандарт и размещения таких изменений (или новых версий Стандарта) на сайте Компании, Подрядчик должен довести такие изменения до своих работников и субподрядчиков под подпись.

Доступ работникам Подрядчика для работы с Информацией Компании предоставляется только после получения Компанией указанных оригиналов обязательств о неразглашении, подписанных работниками Подрядчика.

4. Доступ к Информации

Подрядчик должен обеспечивать, как минимум, следующие меры контроля активации учетной записи, когда Подрядчик обладает Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Компании:

a. Процесс официального утверждения, с тем чтобы предоставление доступа осуществлялось, исходя из рабочей потребности по выполнению должностных обязанностей (т.е. наделение минимальным объемом полномочий, исключительно исходя из необходимого уровня доступа, но не больше).
b. Разделение ответственных между процессами направления запроса, утверждения и предоставления доступа.
c. Учетные записи для доступа к системам, услугам и приложениям должны закрепляться за каждым отдельным пользователем и быть уникальными, а не являться общими.
d. Привилегированные и административные учетные записи должны отличаться от стандартной учетной записи пользователя и иметь уникальные идентификационные данные для входа. Привилегированные учетные записи (с повышенным уровнем доступа, который дает полномочия внутри компьютерной системы, значительно более обширные, чем те, что доступны обычному пользователю) должны предоставляться только ограниченному кругу уполномоченных пользователей.

Контроль паролей должен быть надлежащим образом реализован Подрядчиком, включая следующие требования:

a. Пароли с периодически истекаемым сроком действия.
b. Защищенная передача временных паролей и напоминание о необходимости их замены после первого использования.
c. Замена пароля незамедлительно при возникновении оснований полагать, что учетная запись была скомпрометирована.
d. Пароли общей системы, сервиса и приложения должны меняться каждый раз, когда кто-то, кто знает пароль, либо уходит из организации Подрядчика, либо переходит на другую должность, в рамках которой доступ к системе больше не требуется.
e. Перед сбросом пароля необходимо проверять личность пользователя.
f. Необходимо заменять все пароли, установленные по умолчанию.
g. Требования по надежности пароля должны отвечать общим стандартам безопасности (например, ISO, NIST) в отношении их длины и сложности.

Подрядчик должен применять следующие меры контроля деактивации:

a. Формальный процесс своевременной деактивации учетных записей пользователей, уходящих из организации Подрядчика и (или) больше не испытывающих рабочей потребности входить в систему (например, в течение 24 часов с момента такого события).
b. Процесс, обеспечивающий направление уведомления Компании относительно изменений в составе персонала Подрядчика в течение 24 часов с момента такого события, если такие сотрудники имеют учетные записи или им предоставлен доступ к информационным системам Компании.

Подрядчик должен реализовать следующие средства контроля доступа:

a. Периодические проверки доступа для всех пользователей, системных учетных записей, тестовых учетных записей и общих учетных записей должны производиться и документироваться по меньшей мере раз в год.
b. Учетные записи пользователя должны блокироваться после определенного количества неудачных попыток входа.
c. Учетные записи, по которым в последнее время не было зафиксировано никаких операций (например, за последние 90 дней, за исключением тех, что используются для ежеквартальной, полугодовой и годовой обработки), должны быть отключены.
d. Должны применяться меры контроля сессий, включая блокировку учетной записи и истечение срока сессии.
e. Для любых привилегированных и/или административных учетных записей должна быть предусмотрена многофакторная аутентификация (МФА).
f. Необходимо использовать МФА в отношении любых онлайн-приложений.
g. МФА также применима для всех способов удаленного доступа (например, виртуальных частных сетей, протоколов удаленного рабочего стола).

5. Сетевая и системная безопасность

Подрядчик должен применять, как минимум, следующие меры сетевой и системной безопасности, когда Подрядчик обладает Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Компании:

a. Стандарты защиты операционных систем, приложений и сетевых устройств.
b. Во все системы должны быть внесены соответствующие исправления с учетом обновлений операционной системы и ее основных компонентов в связи с «заплаточным» релизом и оценкой в соответствии с общепринятыми стандартами безопасности (например, ISO, NIST).
c. Исправление уязвимостей онлайн-приложений с высоким уровнем риска должно быть проведено как можно скорее, но не более, чем за 30 дней.
d. Техническое обслуживание систем должно осуществляться на уровне, позволяющем вносить последние обновления/внедрять сервисные пакеты.

Меры контроля сетевой безопасности:

a. Информация, принадлежащая или доверенная Компанией, не должна храниться в демилитаризованной зоне (ДМЗ).
b. На всех сетевых интерфейсах должны быть установлены межсетевые экраны, ограничивающие входящий и исходящий трафик, исходя из текущих потребностей.
c. Необходимо установить системы обнаружения или предупреждения несанкционированного доступа в целях выявления и реагирования на несанкционированное или вредоносное сетевое вторжение.
d. При наличии соглашений об уровне услуг для системы или приложения, заключенных между Компанией и Подрядчиком, должна иметься защита от распределенной атаки типа «отказ в обслуживании» (DDoS-атака).

Меры контроля системной безопасности:

a. Пользовательские устройства (ноутбуки) должны быть зашифрованы и защищены паролем.
b. Корпоративные мобильные устройства (смартфоны, планшеты) должны быть защищены с использованием системы управления мобильными устройствами.
c. Серверы и конечные точки должны быть защищены от воздействия вирусов/вредоносного программного обеспечения, которое подлежит регулярному обновлению.

6. Вход и мониторинг

Операции по входу в информационные системы Подрядчика должны протоколироваться и осуществляться в соответствии с общими стандартами безопасности (например, ISO, NIST). Мониторинг должен, как минимум, выявлять события кибербезопасности и проверять эффективность защитных мер.

7. Управление угрозами и уязвимостями

Подрядчик должен проводить непрерывную оценку уязвимостей и своевременно исправлять проблемы, связанные с приложениями, операционными системами и прочими компонентами инфраструктуры. В дополнение необходимо внедрить сервисы и процессы для выявления, оценки, смягчения и защиты от новых и существующих уязвимостей и угроз безопасности, включая вирусы, боты и прочие вредоносные коды.

Подрядчик должен применять следующие меры контроля:

a. Ежегодные независимые проверки на проникновение в их сети и приложения, отвечающие за обработку Информации.
b. Необходимо проводить ежеквартальный поиск уязвимостей в системе безопасности своих платформ и сетей, которые обрабатывают Информацию, в целях обеспечения соответствия общепринятым стандартам по конфигурированию настроек безопасности платформ и сетей.
c. Риск-ориентированная программа по устранению уязвимостей, направленная на реагирование на результаты проверок на проникновение, уязвимости и оценок нормативно-правового соответствия.
d. При необходимости Подрядчик обеспечит Компании возможность проведения теста защиты информационных систем от несанкционированного доступа.

8. Управление изменениями

Подрядчик должен принять задокументированную политику контроля за внесение изменений, которая включает в себя:

a. Требования к утверждению, классификации, тестированию и испытанию плана восстановления предыдущего состояния.
b. Разделение обязанностей по направлениям: запрос, утверждение и реализация изменений.
c. Управление и обзор экстренных изменений в течение установленного периода (например, 24 часов).

9. Управление активами

Подрядчик должен обеспечивать проведение инвентаризации активов, включая системы/устройства и программное обеспечение, когда Подрядчик обладает Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда у Подрядчика есть удаленное подключение к Среде Компании.

10. Обработка Информации

Подрядчик должен обеспечить отделение Информации от информации прочих клиентов, если у Подрядчика имеется Информация, принадлежащая или доверенная Компанией, находящаяся за пределами Среды Компании, и/или если у Подрядчика есть удаленный доступ к Среде Компании. Кроме того, Подрядчик должен быть способен составить описание прохождения Информации через его Среду.

Электронный обмен информацией между Компанией и Подрядчиком (в том числе по электронной почте, путем передачи файлов, через удаленное подключение и т. д.) должен быть защищен с помощью взаимно согласованных сервисов.

Необходимо использовать процессы и инструменты для обнаружения и реагирования на утечку информации.

Информация не должна храниться или передаваться с использованием портативных устройств хранения без официального разрешения владельца - Компании (полученного посредством процесса направления запроса в Компанию об использовании портативных устройств хранения данных). В случае использования таких устройств вся хранящаяся на них Информация должна быть зашифрована.

11. Шифрование

Необходимо шифровать передаваемую Информацию, если у Подрядчика имеется Информация, принадлежащая или доверенная Компанией, находящаяся за пределами Среды Компании, и/или если у Подрядчика есть удаленный доступ к Среде Компании.

Ключ шифрования, принадлежащий Подрядчику или управляемый Подрядчиком, должен храниться в безопасном месте с контролируемым доступом, а также должна быть подтвержденная возможность восстановления ключа.

Процедуры и процессы шифрования должны соответствовать требованиям общепринятых стандартов по безопасности (например, стандартов ISO, NIST).

12. Физическая безопасность

Необходимо разработать и применять процедуры и физические средства контроля для защиты копий Информации на бумажных носителях и информационных систем (например, аппаратное обеспечение, программное обеспечение, документация и данные), если у Подрядчика имеется Информация, принадлежащая или доверенная компанией, находящаяся за пределами Среды Компании, и/или если у Подрядчика есть удаленный доступ к Среде Компании.

Центры обработки данных должны находиться под физическим контролем, включая формальное управление доступом в зависимости от рабочих потребностей. В Центрах обработки данных должны применяться меры контроля среды (температуры, влажности, резервный источник энергии) в целях предупреждения перебоев или утраты данных.

Подрядчик, который передает, хранит или обрабатывает Информацию, должен проводить ежегодную независимую оценку физической безопасности своих объектов.

13. Непрерывность бизнеса

В дополнение к любым договорным требованиям относительно непрерывности бизнеса и послеаварийного восстановления в случае аварии или перебоев в работе, с учетом прочих требований соглашения и степени критичности Информации, Подрядчик должен гарантировать наличие следующих мер контроля:

a. На объекте первичной обработки данных (входные каналы связи, серверы, терминалы) должно быть в наличии резервное питание и резервные технические возможности обработки.
b. Необходимо обеспечить наличие альтернативной площадки для обработки Информации в целях продолжения рабочих процессов и восстановления функциональности организации Подрядчика в указанный временной период по соглашению, если применимо.
c. Необходимо проводить ежегодные проверки отказоустойчивости в целях демонстрации эффективной способности к непрерывности ведения бизнеса и восстановлению.
d. Требуется осуществлять регулярное резервное копирование применяемых систем и данных в зависимости от уровня критичности. Необходимо периодически проверять данные после резервного копирования на устойчивость к текущим условиям применения.
e. Необходимо обеспечить надлежащую защиту резервных копий и (или) передаваемой информации, а также их хранение отдельно от основного хранилища.

14. Хранение и уничтожение записей

Подрядчик должен хранить Информацию только в течение срока, установленного в соответствующем соглашении, кроме случаев, когда по закону требуется более длительное хранение.

При истечении срока действия договоренности Подрядчик должен вернуть и гарантированно удалить Информацию.

По запросу Компании, Подрядчик должен подтвердить, что Информация была удалена.

15. Управление инцидентами информационной безопасности

Подрядчик должен иметь процедуры управления и реагирования на инциденты в области информационной безопасности (например, раскрытие, нарушение требований конфиденциальности, хищение и т. д.), которые позволяют обоснованно выявлять, расследовать, реагировать, устранять и уведомлять о событиях, которые предполагают наличие определенной угрозы для конфиденциальности, целостности и (или) доступности Информации, когда Подрядчик обладает Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Компании. Процедуры реагирования и управления инцидентами должны документироваться и пересматриваться по меньшей мере раз в год. По запросу Компания должна иметь возможность изучать такие процедуры.

Подрядчик должен уведомлять Компанию о предположительных или известных инцидентах в области информационной безопасности, которые могут оказывать воздействие на Информацию, в течение 24 часов. В дополнение Подрядчик должен использовать задокументированный процесс, включая определенных контактных лиц со стороны Компании и Подрядчика, в целях обеспечения соблюдения данного требования о направлении уведомления.

Подрядчик должен в полной мере сотрудничать с Компанией для прояснения ситуации, понимания ключевых причин и определения необходимых действий для устранения таких причин в случае фактического или предполагаемого инцидента, связанного с информационной безопасностью.

16. Управление субподрядчиками

Настоящий Стандарт информационной безопасности применяется ко всем субподрядчикам, используемым Подрядчиком, которые работают с Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Компании. Подрядчик несет ответственность за то, чтобы обеспечивать уведомление каждого субподрядчика о содержании Стандарта информационной безопасности и его соблюдение таким субподрядчиком. Во избежание сомнений, к субподрядчикам относятся, помимо прочего, подрядчики, оказывающие копировально-множительные услуги, услуги внешнего хранения (архивы), разработчики программного обеспечения, объекты облачного хранения и центры обработки данных.

Подрядчик и субподрядчики должны заключать официальные контракты, в которых описаны необходимые меры контроля, включая меры контроля за обеспечением конфиденциальности, доступности и целостности Информации.

Подрядчику необходимо проводить первоначальные и текущие оценки в целях обеспечения соблюдения субподрядчиками Стандарта информационной безопасности и надлежащего управления происшествиями и проблемами в области безопасности.

Подрядчик должен информировать Компанию и получать письменное одобрение перед использованием услуг субподрядчиков, которые либо намереваются работать с Информацией, либо

будут иметь доступ к системам Подрядчика или Компании, в которых находятся Информация, а также уведомлять Компанию о том, в какой стране(-ах) будет осуществляться работа с Информацией.

17. Право на проверку обеспечения мер Информационной безопасности

Подрядчик должен разрешать Компании и ее агентам, аудиторам (внутренним и внешним), регуляторам и прочим представителям проводить инспектирования, аудиты, изучать и проверять объекты, бухгалтерские книги, системы, записи, реестры доступа, данные, практики и процедуры Подрядчика (и любых субподрядчиков, услуги которых может использовать такое Подрядчик) в целях проверки целостности Информации и мониторинга соблюдения настоящего Стандарта информационной безопасности.

18. Жизненный цикл безопасной разработки системы

Данные требования применимы только к создаваемым Подрядчиком системам, программному обеспечению или приложениям, предназначенным для Компании.

Методология проектирования и разработки программного обеспечения:

a. Определенная методология разработки систем должна быть официально закреплена в тексте политик, процедур и стандартов, подлежащих распространению и соблюдению, и должна соответствовать отраслевым стандартам. Необходимо разработать и довести до сведения соответствующих сотрудников стандарты программирования. Такие стандарты включают в себя спецификации в области архитектуры и дизайна, обзор бизнес-логики, внедрение защитных алгоритмов и библиотек, удаление тестового кода и исправления распространенных ошибок в системе безопасности (см. десять главных уязвимых точек OWASP).
b. Исходный код должен проходить проверки в целях подтверждения соблюдения вышеуказанных стандартов программирования.
c. Использование производственных данных в непроизводственной Среде должно осуществляться только при необходимости. Необходимо применять те же меры контроля безопасности, которые действуют в производственной Среде, или производственная информация, используемая в ходе испытаний, должна быть в достаточной степени замаскирована.
d. Находящееся в открытом доступе программное обеспечение (например, программное обеспечение с открытым кодом, условно-бесплатное и бесплатное программное обеспечение), при использовании такового, должно проходить применимые проверки на предмет потенциального риска, включая потенциальный юридический риск (например, нарушение авторских прав).
e. Находящееся в открытом доступе программное обеспечение (например, программное обеспечение с открытым кодом, условно-бесплатное и бесплатное программное обеспечение), при использовании такового, должно включать меры контроля, гарантирующие, что внедрение такого типа программного обеспечения не окажет отрицательного воздействия (например, вирус, «Троян», нарушения безопасности, такие как «программная закладка»).
f. Исходный код должен храниться в приемлемом для отрасли непубличном средстве управления версиями при наличии строгих средств контроля для проверки исходного кода. Подрядчик должен иметь системы постоянного мониторинга, которые осуществляют мониторинг изменений Среды выполнения кода.
g. Управление жизненным циклом безопасности всего программного обеспечения, как разработанного Подрядчиком, так и приобретенного у третьих лиц.

Версии кода:

a. Подрядчик должен стремиться к непрерывному усовершенствованию выбранной ими модели разработки.
b. Подрядчик должен внедрить и применять официальную политику/процедуру управления изменениями/выпуском в отношении запланированных обновлений программного

обеспечения, которая демонстрирует, что такие выпуски являются запланированными, управляемыми, были проверены, утверждены и надлежащим образом доведены до сведения указанных лиц, при этом Компания должна получать заблаговременные уведомления о запланированных изменениях.

c. Циклы управления изменениями/выпускам начинаются с определения требований. Воздействие, обратная связь и потребность Компании должны быть надлежащим образом интегрированы в требования запланированных выпусков.
d. Регрессивное тестирование должно проводиться в течение каждого цикла выпуска. Тестирование должно проводиться на разных уровнях (например, на уровне единицы, интеграции и системы, пользователя). В основе пользовательского тестирования должны лежать официальные планы испытаний, проводимых лицами, которые никоим образом не зависят от тех, кто отвечает за проектирование и разработку системы.
e. Необходимо получать официальные одобрения на каждом этапе жизненного цикла разработки (определение требований, проектирование, тестирование, приемка пользователем, реализация производства и т. д.). При регистрации одобрений должно быть понятно, кто, когда и в отношении чего выдает одобрение.
f. Релизы и патчи должны предоставляться с достаточным объемом указаний по их развертыванию и (или) использованию. К ним относятся такие решения, когда Компания сама предоставляет релиз или патч для использования, а также решения, когда Компанию уведомляют об изменении, которое Подрядчик внес в Среду Компании.

Промежуточные изменения/Исправления ошибок:

a. Должна быть в наличии процедура внесения экстренных изменений/устранения ошибок, в том числе для устранения уязвимостей безопасности, для гарантии того, что такие изменения могут быть внесены своевременно, но при этом контролируемо
b. Должен существовать официальный процесс по уведомлению Компании об известных ошибках и дефектах.
c. Изменения, вносимые в связи с исправлением ошибок, должны подлежать официальной проверке и демонстрировать надлежащее документирование и утверждение. Утверждение должно проводиться лицом, отличным от сотрудника, вносящего изменение.