ОБЩИЕ ТРЕБОВАНИЯ О КИБЕРБЕЗОПАСНОСТИ

Настоящий документ устанавливает обязательные требования и рекомендации, предъявляемые YADRO к Компаниям (к третьим лицам/поставщикам/подрядчикам) необходимые для обеспечения информационной безопасности и защиты интересов YADRO при использовании Компаниями информационных активов YADRO и исполнении заключенных Договоров.

Настоящие требования распространяются на все виды взаимодействия, за исключением договоров, заключаемых в целях предоставления труда работников (персонала). Указанные договоры регулируются отдельными условиями, с учетом требований законодательства Российской Федерации и специфики оказания услуг по предоставлению персонала.

Термины, определения и сокращения

Авторизация — процесс предоставления прав субъекту доступа для выполнения определенных операций над объектами доступа в информационных системах.

ДИБ — Департамент информационной безопасности YADRO, структурное подразделение, ответственное за обеспечение информационной безопасности в YADRO.

Договор — любой Договор, Сделка, Контракт или иное Соглашение между YADRO и Компанией.

YADRO — Сторона 1 (YADRO).

Компания — Сторона 2 (контрагент YADRO по Договору).

ИБ (Информационная Безопасность) — состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Информационный актив, ИА — информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для YADRO, находящаяся в распоряжении YADRO и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Информация ограниченного доступа — любая информация, доступ к которой ограничен федеральным законодательством Российской федерации и локальными нормативными актами YADRO.

Инцидент ИБ — непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (может привести) к нарушению функционирования IT-ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационной безопасности.

IT-ресурсы — оборудование, программное обеспечение, сети и другие системы, предназначенные для хранения, обработки и передачи информации YADRO.

Композиционный анализ — метод анализа исходного кода программного обеспечения для выявления используемых сторонних библиотек и компонентов, в том числе с открытым исходным кодом, с целью проверки их на наличие уязвимостей, соответствие лицензиям и другим критериям безопасности.

Конфиденциальная информация — информация, доступ к которой ограничен в соответствии с законодательством Российской Федерации и внутренними нормативными документами YADRO, а также любые данные, доступ к которым предоставлен Компании в рамках выполнения обязательств по Договору и которые не подлежат разглашению без согласия YADRO.

ЛВС — локальная вычислительная сеть.

ПДн (Персональные данные) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

ПМИ (Программа и методика испытаний) — технический документ, который содержит данные (характеристики, параметры, свойства, показатели), подлежащие проверке при проведении испытаний изделия, а также порядок и методы их контроля.

Процедура аудита информационной безопасности — процесс проверки соответствия мер информационной безопасности требованиям, установленным законодательством, нормативными документами и внутренними стандартами YADRO.

ПСИ (Приемосдаточные Испытания) — проверка программного обеспечения или системы на соответствие требованиям после выполнения всех установленных разработчиком и YADRO процедур разработки, тестирования и исправления ошибок.

РБПО (Разработка Безопасного Программного Обеспечения) — процесс разработки программного обеспечения с учетом требований безопасности, включающий использование методик и инструментов для предотвращения возникновения уязвимостей на этапе разработки.

Риск — мера, учитывающая вероятность реализации угрозы и размер ущерба от реализации этой угрозы.

Риск ИБ — риск, связанный с угрозой ИБ.

ПО — программное обеспечение.

Угроза ИБ — угроза нарушения свойств ИБ — доступности, целостности, конфиденциальности информационных активов YADRO.

Удаленный доступ — процесс предоставления Компании возможности подключаться к IT-ресурсам YADRO с использованием удаленных средств (например, через VPN, терминальные подключения) для выполнения работ в рамках Договора.

Ущерб — утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры YADRO или другой вред активам и (или) инфраструктуре YADRO, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Цепочка поставок — совокупность процессов и участников (включая разработчиков, поставщиков и подрядчиков), задействованных в создании, поставке и обслуживании программного обеспечения или оборудования, используемого YADRO.

Шифрование — процесс преобразования информации в код, который невозможно прочитать без специальных средств (ключей шифрования), с целью защиты конфиденциальной информации при передаче или хранении.

IDS (Intrusion Detection System) — система обнаружения вторжений, которая анализирует сетевой трафик и выявляет подозрительные или вредоносные действия, но не блокирует их, а только уведомляет об инциденте.

IPS (Intrusion Prevention System) — система предотвращения вторжений, предназначенная для активного блокирования вредоносных действий в сетях и на хостах путем фильтрации и анализа трафика.

SBOM (Software Bill of Materials) — перечень всех программных компонентов, используемых в разработке программного обеспечения, включая компоненты с открытым исходным кодом и сторонние библиотеки, с указанием их версий и источников.

1. Предмет Требований

1.1. Настоящие требования по информационной безопасности (далее — «Требования о ИБ») определяют обязательные для Компаний (третьих лиц / поставщиков / подрядчиков) меры и рекомендации по информационной безопасности, предъявляемые при выполнении Компаниями работ в сфере информационных технологий и/или информационной безопасности, а также при предоставлении Компаниям доступа к IT-ресурсам YADRO. Положения настоящих требований по информационной безопасности применяются в той части, в которой они напрямую применимы и относятся к конкретным видам работ или услуг, выполняемых (оказываемых) Компанией по договорам с YADRO. Указанные Требования о ИБ не являются исчерпывающими и могут быть дополнены или уточнены с учётом характера оказываемых услуг, выполняемых работ и специфики деятельности Компании.

2. Общие положения

2.1. В случае выполнения Компанией работ, оказания услуг в сфере информационных технологий и/или информационной безопасности, а также при предоставлении Компании удаленного доступа к IT-ресурсам YADRO, применяются требования к обеспечению информационной безопасности (Далее — «Требования ИБ»).

2.2. Компания гарантирует, что исполнение условий Договоров с YADRO не приведет к появлению скрытых функциональных возможностей (незадекларированных изменений, операций или внедренных «программных закладок»).

2.3. При выполнении Компанией поставки ПО, ПО должно обеспечивать реализацию следующих мер безопасности:

2.3.1. В ПО должна быть реализована ролевая модель разграничения доступа для пользователей и обслуживающего персонала. Различным пользователям и/или группам пользователей должны назначаться различные права доступа в Систему, в рамках их должностных обязанностей, а также с соблюдением принципов «минимально необходимых привилегий» и «минимально необходимых знаний» (для выполнения их должностных обязанностей).

2.3.2. ПО должно обеспечивать возможность журналирования и хранения действий пользователей, включая попытки (как успешные, так и не успешные) авторизации и изменения объектов системы (изменения учетных данных и прав доступа), доступа к ключевым функциям системы.

2.3.3. В ПО должна быть реализована функциональность идентификации и аутентификации пользователей через систему управления доступом (IAM), например, Keycloak или аналогичные решения, поддерживающие протоколы OpenID Connect и SAML. В ПО должна быть реализована функциональность идентификации и аутентификации пользователей с использованием корпоративной службы каталогов (например, Active Directory, LDAP). Для доступа к ИС должен быть предусмотрен механизм единого входа — SSO (single sign-on).

2.3.4. Все конфиденциальные данные, передаваемые и хранимые в ПО, должны быть зашифрованы с использованием современных алгоритмов шифрования для защиты от несанкционированного доступа.

2.3.5. На момент передачи ПО в YADRO Компания гарантирует отсутствие уязвимостей в ПО. В случае выявления YADRO уязвимостей в ПО, Компания обязуется устранить их до ввода ПО в опытно-промышленную эксплуатацию за свой счет.

2.3.6. ПО должно быть совместимо с современными средствами антивирусной защиты, производимых на территории Российской Федерации (в т.ч., Kaspersky Endpoint Security).

3. Общие положения

3.1. В случае, если условия Договора включают право привлечения Компанией третьих лиц, то соблюдаются следующие условия:

3.1.1. Компания несет полную ответственность за привлекаемых третьих лиц, включая выполнение ими требований настоящего Соглашения о ИБ и соблюдение мер информационной безопасности, установленных YADRO настоящим Соглашением о ИБ.

3.1.2. Категорически запрещено самостоятельное подключение Компанией третьих лиц к ИТ-инфраструктуре YADRO без письменного согласования YADRO.

4. Удаленный доступ

4.1. Компании может быть предоставлен удаленный доступ к IT-ресурсам YADRO исключительно в целях исполнения Договора и на срок его действия. Удаленный доступ предоставляется на срок не более 1 (одного) года. При необходимости продления доступа, удаленный доступ оформляется повторно. По окончании действия или досрочном расторжении Договора, доступ прекращается.

4.2. Доступ предоставляется только в случае наличия подписанного Соглашения о неразглашении информации, а также Соглашения о доступе, в котором перечислены IT-ресурсы, к которым требуется доступ.

4.3. При предоставлении удаленного доступа к IT-ресурсам YADRO Компания:

4.3.1. Обязана соблюдать условия получения удаленного доступа к IT-ресурсам YADRO.

4.3.2. Не предоставлять третьим лицам доступ без предварительного письменного согласия YADRO.

4.3.3. Не раскрывать и не передавать такую информацию третьим лицам без получения предварительного письменного согласия YADRO.

4.4. Удаленный доступ к IT-ресурсам YADRO, содержащим персональные данные, предоставляется только при соблюдении требований действующего законодательства Российской Федерации в области защиты персональных данных, а также соответствующих условий Договора.

4.5. Уведомления и сообщения в рамках настоящих Требований ИБ направляются Сторонами в соответствии с условиями, указанными в Договоре.

4.6. Компания должна иметь базовые политики и процедуры в области информационной безопасности, направленные на защиту конфиденциальности, целостности и доступности информации, включая:

a. использование средств антивирусной защиты и управления доступами;
b. установку паролей на устройствах учетных записях;
c. идентификацию и аутентификацию пользователей;
d. уведомление YADRO об инцидентах Информационной безопасности.

4.7. В целях обеспечения информационной безопасности YADRO оставляет за собой право в одностороннем порядке блокировать учетные записи и доступы Компании в случае возникновения инцидентов информационной безопасности.

4.8. До предоставления доступа к ресурсам YADRO Компания обязана ознакомить своих сотрудников (и третьих лиц, если они привлекаются) с настоящими требованиями. Ответственность за ознакомление сотрудников (и третьих лиц, если они привлекаются) лежит на Компании.

4.9. Уволенные сотрудники Компании, а также сотрудники, снятые с проекта или утратившие необходимость доступа к ресурсам YADRO, должны быть лишены доступа к ресурсам YADRO со дня увольнения, перевода на другую работу, снятия с проекта или прекращения их участия в работах по Договору. Компания несет ответственность за своевременное уведомление YADRO не позднее 1 (одного) рабочего дня до дня увольнения, снятия с проекта или перевода сотрудника, чтобы YADRO мог предпринять соответствующие меры по прекращению доступа сотрудника Компании.

5. Безопасность рабочих мест

5.1. Для удаленного доступа к IT-ресурсам YADRO Компания обязана использовать ПО для удаленного подключения, рекомендованное YADRO и с использованием конфигураций, предоставленных YADRO.

5.2. Компания обязана использовать на всех ИТ-активах (пользовательские компьютеры/автоматизированные рабочие места, серверы, информационные системы и пр.) для удаленного доступа к IT-ресурсам YADRO только лицензионное и официально приобретенное антивирусное ПО и поддерживать его в актуальном состоянии, включая актуализацию антивирусных баз.

5.3. Компания обязуется поддерживать все ИТ-активы (пользовательские компьютеры/ автоматизированные рабочие места, серверы, информационные системы и пр.) для удаленного доступа к IT-ресурсам YADRO в актуальном состоянии, регулярно устанавливая обновления и патчи, обеспечивающие устранение известных уязвимостей в операционных системах и ПО.

5.4. Права сотрудника на рабочем месте, с которого осуществляется удаленный доступ к IT-ресурсам YADRO, должны быть организованы с учетом мер информационной безопасности и не позволять осуществлять действия, которые могут нарушить работоспособность или защиту программно-аппаратного обеспечения YADRO, в том числе внесение изменений, не предусмотренных условиями Договора. При этом права сотрудников не должны ограничивать их работу, необходимую для исполнения условий Договора.

5.5. В случае предоставления YADRO средств вычислительной техники в рамках выполнения работ, оказания услуг в сфере информационных технологий и/или информационной безопасности, а также при предоставлении Компании удаленного доступа к IT-ресурсам YADRO Компании запрещается:

a. предпринимать попытки преодоления установленных YADRO ограничений, отключать и/или удалять установленные на предоставленных средств вычислительной техники YADRO средства защиты информации (в том числе антивирусное ПО), использовать недокументированные свойства, ошибки в ПО и настройках защиты доступа к IT-ресурсам и ИС YADRO, доступ к которым не был предоставлен явным образом;

b. не устанавливать на предоставленные средства вычислительной техники YADRO какое-либо ПО, изменять настройки уже имеющегося. По вопросам установки необходимого ПО, а также получения административных прав в операционных системах персональных компьютеров обращаться в отдел информационных технологий YADRO;

c. не организовывать на предоставленном средстве вычислительной техники ресурсы общего доступа и сетевые сервисы (открывать доступ к общим папкам, дискам, CD-приводам и дисководам, настраивать службы удаленного доступа, прокси- или веб-серверы, беспроводные точки доступа, Bluetooth интерфейсы и т.д.);

d. не хранить и не использовать на предоставленном компьютере ПО и другие результаты интеллектуальной деятельности в нарушение прав их законных правообладателей;

e. не подключать к предоставленным средствам вычислительной техники YADRO мобильные устройства (телефоны, смартфоны, планшетные компьютеры, ноутбуки), беспроводные (радио) интерфейсы, модемы и прочее оборудование, позволяющее выходить в сеть Интернет и другие публичные сети.

5.5.1. Не использовать без письменного согласования ПО следующих категорий при подключении к корпоративной сети YADRO:

a. сканеры портов и анализаторы трафика;

b. средства для организации удаленного доступа, не утвержденные письменно YADRO, включая средства для создания зашифрованных каналов связи (VPN-, DNS-, SSH-, HTTPS-туннели и пр.);

c. ПО, используемое для анонимного доступа в сеть Интернет (включая веб-сервисы, прокси-серверы);

d. ПО для обхода средств защиты, включая средства подбора и восстановления паролей, поиска уязвимостей;

e. ПО, предназначенное для сокрытия или внедрения дополнительной информации в цифровые объекты (в том числе реализующее методы стеганографии);
f. ПО, осуществляющее сбор информации с клавиатуры, экрана, микрофона (снифферы);
g. специализированные программные средства, оказывающее влияние на сетевые настройки средств вычислительной техники, серверов и сетевого оборудования.

Исключение
Допускается использование данных категорий ПО (указанных в п.5.5, 5.5.1 настоящих Требований о ИБ) для целей исполнения Договора, если использование таких средств прямо предусмотрено его предметом или рамками оказания услуг Компанией.

6. Контроль состояния ИБ и реагирование на инциденты информационной безопасности

6.1. Компания гарантирует отсутствие уязвимостей информационной безопасности в ПО. На момент передачи ПО в нем должны отсутствовать уязвимости информационной безопасности уровня CVSS > 5.

6.2. Компания обязуется регулярно проводить оценку уязвимостей (не реже одного раза в квартал) и своевременно устранять выявленные уязвимости в ПО в период действия гарантийной поддержки.

6.3. При выявлении уязвимостей в ПО одной из Сторон, Стороны обязуются своевременно, но не позднее 3 (трех) рабочих дней, с момента выявления уязвимости, информировать друг друга.

6.4. Компания устраняет выявленные YADRO в коде ПО, обновлений ПО уязвимости — со степенью критичности «критический» — не позднее 14 (четырнадцати) дней с момента уведомления, со степенью критичности «высокий» — не позднее 30 (тридцати) дней с даты уведомления, со степенью критичности «средний» — не позднее 90 (девяносто) дней с даты уведомления, со степенью критичности «низкий» — в порядке, определенном YADRO.

6.5. Компания несет ответственность за исправление уязвимостей независимо от их происхождения, включая уязвимости, обнаруженные в модулях сторонних вендоров, используемых в ПО. Это требование необходимо для обеспечения безопасности конечного продукта и защиты цепочки поставок.

6.6. В случае возникновения инцидента ИБ на стороне Компании, который мог привести к компрометации ПО и сред его разработки, Компания обязуется не позднее 3 (трех) рабочих дней с момента выявления инцидента ИБ предоставить YADRO следующую информацию в объеме, не содержащем конфиденциальные сведения: описание инцидента, его причины, возможные последствия для YADRO, а также меры, принятые для предотвращения аналогичных инцидентов в будущем.

6.7. Компания обязуется проводить регулярные оценки уязвимостей своих систем и своевременно устранять обнаруженные угрозы безопасности.

6.8. Компания на постоянной основе, не реже одного раза в год, должна проводить сканирование защищенности внешнего периметра ЛВС (при наличии у Компании внешнего периметра ЛВС). Сканирование может осуществляться как сторонней аккредитованной организацией, имеющей право проведения подобных работ, так и самим Компанией при соблюдении следующих условий:
a. в случае проведения сканирования защищенности силами Компании, проверка должна быть проведена в соответствии с установленными стандартами в области информационной безопасности;
b. компания обязана документировать процедуру сканирования, составлять отчеты о результатах проверки;
c. область сканирования должна включать, как минимум, средства вычислительной техники и сетевое оборудование, взаимодействующее с инфраструктурой YADRO, а также сетевой трафик устройств, обрабатывающих данные клиентов или партнеров YADRO.

6.9. Компания должна иметь внедренные процедуры для выявления и устранения уязвимостей, связанных с приложениями и операционными системами, с учётом стандартов серии ISO и других международных практик по информационной безопасности.

6.10. Компания обязана безотлагательно предпринимать все необходимые меры по предотвращению и минимизации ущерба, нанесенного YADRO при возникновении инцидентов информационной безопасности, и по запросу YADRO предоставлять отчеты по их результатам.

6.11. В случае возникновения / выявления инцидентов информационной безопасности Компания обязана незамедлительно уведомить YADRO и провести все необходимые действия и проверки самостоятельно или с привлечением YADRO для устранения инцидента и его последствий.

7. Требования к средам разработки и тестирования

7.1. Требования к Компании, поставляющей ПО в виде исходного кода, программных продуктов, развертываемых на инфраструктуре YADRO, которые поставляют программный Продукт в виде исходного кода, в отношении:

a. реализации процессов разработки Компании;
b. передачи исходного кода Продукта и исходного кода обновлений Продукта от Компании YADRO;
c. сборки и тестирования кода YADRO;
d. устранения уязвимостей в коде, переданном YADRO Компанией;
e. доступа Компании к средам разработки и тестирования YADRO;
f. лицензионной чистоты.

7.2. Общие требования:

a. Компания должна передать YADRO заверенные соответствующим руководителем подразделения разработки Компании описание средств разработки и тестирования ПО с указанием производителя и версии средств разработки, описание средств управления конфигурацией ПО в средах разработки и тестирования.
b. Все технические средства Компании, используемые в разработке ПО, включая среды разработки и тестирования, репозитории программного кода, репозитории программных компонентов, системы управления CI/CD, должны находиться в пределах Российской Федерации.

7.3. Требования по передаче кода Продукта и кода обновлений Продукта от Компании YADRO:

7.3.1. Компания должна предоставить доступ YADRO к исходному коду Продукта одним из следующих способов:

a. Компания предоставляет YADRO учетные записи в репозиториях Компании, в которых размещен исходный код. Компания должна поддерживать указанные репозитории и обеспечивать доступ к ним на протяжении всего срока действия Договора и дополнительных соглашений к нему, а также Договоров и соглашений о технической поддержке. Данное положение включает своевременное обновление содержимого репозиториев, предоставление необходимых прав доступа YADRO и обеспечение бесперебойной работы репозиториев Компании.
b. YADRO предоставляет Компании учетные записи в системе управления репозиториями YADRO к соответствующей группе репозиториев. Компания размещает исходный код Продукта в репозиториях YADRO.

7.3.2. Каждое изменение исходного кода компонентов Продукта должно быть отмечено тегом с номером версии Продукта с использованием семантического версионирования.

7.3.3. Компания должна предоставить доступ YADRO ко всем необходимым для сборки Продукта компонентам и исполняемым модулям ПО, заимствованным у сторонних разработчиков (в т.ч. компонентам с открытым исходным кодом), а также системным обновлениям. Компания предоставляет YADRO учетные записи в репозиториях программных компонентов Компании, в которых размещаются указанные компоненты и обновления. Компания должна поддерживать указанные репозитории и обеспечивать доступ к ним на протяжении всего срока действия Договора

и дополнительных соглашений к нему, а также Договоров и соглашений о технической поддержке. Данное положение включает своевременное обновление содержимого репозиториев, предоставление необходимых прав доступа YADRO и обеспечение бесперебойной работы репозиториев Компании и доступность в репозиториях Компании всех необходимых для сборки Продукта компонентов.

7.3.4. Компания передает YADRO руководство по сборке и развертыванию Продукта на инфраструктуре YADRO. Руководство должно содержать исчерпывающие сведения для сборки, установки и настройки продукта на инфраструктуре YADRO. При невозможности сборки и развертывания Продукта на инфраструктуре YADRO в соответствии с руководством Компании, Компания своевременно корректирует руководство и направляет YADRO.

7.3.5. По сборке и тестированию кода YADRO:

a. Запрещается использование для сборки Продукта исходного кода, программных компонентов, заимствованных у сторонних разработчиков (в т.ч. компонентов с открытым исходным кодом), размещенных в публичных репозиториях исходного кода, репозиториях исходного кода сторонних разработчиков и публичных репозиториях программных компонентов, репозиториях программных компонентов сторонних разработчиков.
b. YADRO проводит анализ кода Продукта на наличие потенциальных уязвимостей. YADRO проводит следующие виды анализа кода: статический анализ исходного кода Продукта, композиционный анализ кода продукта, динамический анализ кода продукта, в т.ч. тестирование на проникновение.
c. YADRO проводит все указанные виды анализа кода при каждой передаче кода Компанией.
d. При отсутствии изменений кода YADRO проводит композиционный анализ кода не реже одного раза в квартал.
e. Все указанные виды анализа кода являются частью ПМИ и ПСИ на каждом из этапов передачи результатов работ Компанией.
f. YADRO проводит оценку результатов анализа кода и устанавливает степень критичности выявленных в процессе анализа кода недостатков (потенциальных уязвимостей); CVSS ≥ 9 — «критический», CVSS ≥ 7 — «высокий», CVSS ≥ 5 — «средний», остальные — «низкий»).

7.3.6. По сборке и тестированию кода YADRO:

a. YADRO уведомляет Компанию о выявлении в поставленном ПО потенциальных уязвимостей с описанием и указанием степени критичности каждой уязвимости.
b. Компания устраняет выявленные уязвимости — со степенью критичности «критический» — не позднее 14 (четырнадцати) дней с момента уведомления, со степенью критичности «высокий» — не позднее 30 (тридцати) дней с даты уведомления, со степенью критичности «средний» — не позднее 90 (девяносто) дней с даты уведомления, со степенью критичности «низкий» — в порядке, определенном Компанией.

7.3.7. Требования к доступу Компании в среды разработки, тестирования и продуктивную среду Продукта в инфраструктуре YADRO:

a. Сотрудники Компании не могут иметь доступа к любым сетям, средам, интегрируемым системам, в которых содержатся продуктивные данные.
b. Для разбора ошибок, возникающих в продуктивных средах и интегрируемых системах, YADRO передает Компании журналы/логи указанных систем.
c. В случае необходимости использования в средах разработки и тестирования персональных данных, Компания должна предоставить YADRO инструкцию по обезличиванию персональных данных, которые могут обрабатываться в Продукте (на тестовых стендах)).
d. Доступ сотрудникам Компании к средам разработки и тестирования предоставляется на основе учетной записи в Active Directory YADRO. Такая учетная запись выдается сотруднику Компании на основании запроса сотрудника владельца соответствующей среды. Выданная учетная запись предоставляет доступ к средам разработки и тестирования в соответствии с ролью сотрудника Компании.

7.3.8. Требования лицензионной чистоты:

a. Сборка продукта из исходного кода и программных компонентов, поставляемых Компанией, не должна создавать для YADRO обязательств по приобретению прав на ПО/компоненты ПО сторонних производителей.

7.4. Требования к Компании, поставляющей ПО в форме Дистрибутива и расширений в виде исходного кода, программных продуктов, развертываемых на инфраструктуре YADRO, которые поставляют программный Продукт в форме Дистрибутива и Расширений продукта в отношении:

a. реализации процессов разработки Компании;
b. передачи кода Продукта и кода обновлений Продукта от Компании YADRO;
c. передачи исходного кода Расширений Продукта от Компании YADRO;
d. сборки и тестирования кода YADRO;
e. устранения уязвимостей в коде, переданном YADRO Компанией;
f. доступ Компании к средам разработки и тестирования YADRO;
g. лицензионной чистоты.

7.4.1. Общие определения:

a. Дистрибутив — набор модулей Продукта, поставляемых в виде бинарного кода и обновляемый в рамках релизной политики Продукта.
b. Расширения продукта – набор модулей продукта, поставляемых в виде исходного кода, разрабатываемый и обновляемый в рамках соглашений с YADRO.

7.4.2. Общие требования:

a. Компания должна передать YADRO заверенные соответствующим руководителем подразделения разработки описание средств разработки и тестирования ПО с указанием производителя и версии средств разработки, описание средств управления конфигурацией ПО в средах разработки и тестирования.
b. Все технические средства Компании, используемые в разработке ПО, включая среды разработки и тестирования, репозитории программного кода, репозитории программных компонентов, системы управления CI/CD, должны находиться в пределах Российской Федерации.

7.4.3. Требования по передаче кода Продукта и кода обновлений Продукта от Компании YADRO:

7.4.3.1. Компания предоставляет YADRO учетные записи в репозиториях Компании, в которых размещен код Продукта и обновлений Продукта. Компания должна поддерживать указанные репозитории и обеспечивать доступ к ним на протяжении всего срока действия Договора и дополнительных соглашений к нему, а также Договоров и соглашений о технической поддержке. Данное положение включает своевременное обновление содержимого репозиториев, предоставление необходимых прав доступа YADRO и обеспечение бесперебойной работы репозиториев Компании.

7.4.3.2. Компания должна предоставить доступ YADRO к исходному коду Расширений Продукта одним из следующих способов:

a. Компания предоставляет YADRO учетные записи в репозиториях Компании, в которых размещен исходный код Расширений Продукта, разрабатываемых Компанией по соглашению с YADRO. Компания должна поддерживать указанные репозитории и обеспечивать доступ к ним на протяжении всего срока действия Договора и дополнительных соглашений к нему, а также Договоров и соглашений о технической поддержке. Данное положение включает своевременное обновление содержимого репозиториев, предоставление необходимых прав доступа YADRO и обеспечение бесперебойной работы репозиториев Компании.
b. YADRO предоставляет Компании учетные записи в системе управления репозиториями YADRO к соответствующей группе репозиториев. Компания размещает исходный код Расширений Продукта в репозиториях YADRO.

7.4.3.3. Каждое изменение исходного кода Расширений Продукта должно быть тегировано номером версии Продукта с использованием семантического версионирования.

7.4.3.4. При каждой передаче кода Продукта Компания должна передать вместе с Продуктом перечень используемых в Продукте заимствованных у сторонних разработчиков компонентов (в т.ч. компонентов с открытым исходным кодом) – SBOM (software bill of materials) в формате CycloneDX 1.6.

7.4.3.5. Компания должна предоставить доступ YADRO ко всем необходимым для сборки Расширений Продукта компонентам и исполняемым модулям ПО, заимствованным у сторонних разработчиков (в т.ч. компонентам с открытым исходным кодом), а также системным обновлениям. Компания предоставляет YADRO учетные записи в репозиториях программных компонентов Компании, в которых размещаются указанные компоненты и обновления. Компания должна поддерживать указанные репозитории и обеспечивать доступ к ним на протяжении всего срока действия Договора и дополнительных соглашений к нему, а также Договоров и соглашений о технической поддержке. Данное положение включает своевременное обновление содержимого репозиториев, предоставление необходимых прав доступа YADRO и обеспечение бесперебойной работы репозиториев Компании и доступность в репозиториях Компании всех необходимых для сборки Расширений Продукта компонентов.

7.4.3.6. Компания должна передать YADRO руководство по развертыванию Продукта, а также по сборке и развертыванию Расширений и обновлений Продукта на инфраструктуре YADRO. Руководство должно содержать исчерпывающие сведения для сборки, установки и настройки Продукта, Расширений и обновлений Продукта на инфраструктуре YADRO. При невозможности сборки и развертывания Продукта, Расширений и обновлений Продукта на инфраструктуре YADRO в соответствии с руководством Компании, Компания своевременно корректирует руководство и направляет YADRO.

7.4.4. Требования по устранению потенциальных уязвимостей в коде, переданном YADRO Компанией:

a. YADRO уведомляет Компанию о выявлении в поставленном ПО потенциальных уязвимостей с описанием и указанием степени критичности каждой уязвимости.

b. Компания устраняет выявленные YADRO в коде Продукта, Расширений Продукта, обновлений Продукта уязвимости — со степенью критичности «критический» — не позднее 14 (четырнадцати) дней с момента уведомления, со степенью критичности «высокий» — не позднее 30 (тридцати) дней с даты уведомления, со степенью критичности «средний» — не позднее 90 (девяносто) дней с даты уведомления, со степенью критичности «низкий» — в порядке, определенном Компанией.

c. YADRO уведомляет Компанию о выявлении в Продукте, обновлении Продукта, компонентов, заимствованных у сторонних разработчиков, не перечисленных в SBOM.

d. При обнаружении YADRO в коде Продукта, коде обновления Продукта, компонентов, заимствованных у сторонних разработчиков, не перечисленных в SBOM, Компания должна передать YADRO обновление SBOM не позднее 14 (четырнадцати) дней с момента уведомления.

7.4.5. Требования к доступу Компании в среды разработки, тестирования и продуктивную среду Продукта в инфраструктуре YADRO:

a. Сотрудники Компании не могут иметь доступа к любым сетям, средам, интегрируемым системам, в которых содержатся продуктивные данные.

b. Для разбора ошибок, возникающих в продуктивных средах и интегрируемых системах, YADRO передает Компании журналы/логи указанных систем.

c. В случае необходимости использования в средах разработки и тестирования персональных данных, Компания должна предоставить YADRO инструкцию по обезличиванию персональных данных, которые могут обрабатываться в Продукте.

d. Доступ сотрудникам Компании к средам разработки и тестирования предоставляется на основе учетной записи в Active Directory YADRO. Такая учетная запись выдается сотруднику Компании на основании запроса сотрудника владельца соответствующей среды. Выданная учетная запись предоставляет доступ к средам разработки и тестирования в соответствии с ролью сотрудника Компании.

7.4.6. Требования лицензионной чистоты:

a. Сборка Расширений Продукта из исходного кода и программных компонентов, поставляемых Компанией, не должна создавать для YADRO обязательств по приобретению прав на ПО/компоненты ПО сторонних производителей.

7.4. Требования к Компании, поставляющей ПО в форме Дистрибутива в отношении:

a. реализации процессов разработки Компании;
b. передачи кода Продукта и кода обновлений Продукта от Компании YADRO;
c. тестирования кода YADRO;
d. устранения уязвимостей в коде, переданном YADRO Компанией;
e. доступу Компании к средам разработки и тестирования YADRO.

7.5.1. Общие определения:

a. Дистрибутив — набор модулей Продукта, поставляемых в виде бинарного кода и обновляемый в рамках релизной политики Продукта.

7.5.2. Общие требования:

a. Компания должна передать YADRO заверенные соответствующим руководителем подразделения разработки описание средств разработки и тестирования ПО с указанием производителя и версии средств разработки, описание средств управления конфигурацией ПО в средах разработки и тестирования.
b. Все технические средства Компании, используемые в разработке ПО, включая среды разработки и тестирования, репозитории программного кода, репозитории программных компонентов, системы управления CI/CD, должны находиться в пределах Российской Федерации.

7.5.3. Требования по передаче кода Продукта и кода обновлений Продукта от Компании YADRO:

a. Компания предоставляет YADRO учетные записи в репозиториях Компании, в которых размещен код Продукта и обновлений Продукта. Компания должна поддерживать указанные репозитории и обеспечивать доступ к ним на протяжении всего срока действия Договора и дополнительных соглашений к нему, а также Договоров и соглашений о технической поддержке. Данное положение включает своевременное обновление содержимого репозиториев, предоставление необходимых прав доступа YADRO и обеспечение бесперебойной работы репозиториев Компании.
b. При каждой передаче кода Продукта Компания должна передать вместе с Продуктом перечень используемых в Продукте заимствованных у сторонних разработчиков компонентов (в т.ч. компонентов с открытым исходным кодом) — SBOM (software bill of materials) в формате CycloneDX 1.6.
c. Компания должна передать YADRO руководство по развертыванию Продукта и обновлений Продукта на инфраструктуре YADRO. Руководство должно содержать исчерпывающие сведения для сборки, установки и настройки Продукта и обновлений Продукта на инфраструктуре YADRO. При невозможности сборки и развертывания Продукта обновлений Продукта на инфраструктуре YADRO в соответствии с руководством Компании, Компания своевременно корректирует руководство и направляет YADRO.

7.5.4. Требования по тестированию кода YADRO:

a. Запрещается использовать для развертывания Продукта и обновлений Продукта, исходный код, программные компоненты, заимствованные у сторонних разработчиков (в т.ч. компоненты с открытым исходным кодом), размещенные в публичных репозиториях программных компонентов, репозиториях программных компонентов сторонних разработчиков.
b. YADRO проводит анализ кода Продукта на наличие потенциальных уязвимостей. YADRO проводит следующие виды анализа кода: композиционный анализ кода Продукта, динамический анализ кода Продукта и тестирование на проникновение.
c. YADRO проводит все указанные виды анализа кода при каждой передаче кода Компанией.
d. При отсутствии изменений кода YADRO проводит композиционный анализ кода не реже одного раза в квартал.
e. Все указанные виды анализа кода являются частью ПМИ и ПСИ на каждом из этапов передачи результатов работ Компанией.
f. YADRO проводит оценку результатов анализа кода и устанавливает степень критичности выявленных в процессе анализа кода недостатков (потенциальных уязвимостей). CVSS ≥ 9 — «критический», CVSS ≥ 7 — «высокий», CVSS ≥ 5 — «средний», остальные — «низкий»).

7.5.5. Требования по устранению потенциальных уязвимостей в коде, переданном YADRO Компанией:

a. YADRO уведомляет Компанию о выявлении в поставленном ПО потенциальных уязвимостей с описанием

и указанием степени критичности каждой уязвимости.

b. Компания устраняет выявленные YADRO в коде Продукта, обновлений Продукта уязвимости — со степенью критичности «критический» — не позднее 14 (четырнадцати) дней с момента уведомления, со степенью критичности «высокий» — не позднее 30 (тридцати) дней с даты уведомления, со степенью критичности «средний» — не позднее 90 (девяносто) дней с даты уведомления, со степенью критичности «низкий» — в порядке, определенном Компанией.

c. YADRO уведомляет Компанию о выявлении в Продукте, обновлении Продукта, компонентов, заимствованных у сторонних разработчиков, не перечисленных в SBOM.

d. При обнаружении YADRO в коде Продукта, обновлениях Продукта, компонентов, заимствованных у сторонних разработчиков, не перечисленных в SBOM, Компания должна передать YADRO обновление SBOM не позднее 14 (четырнадцати) дней с момента уведомления.

7.5.6. Требования к доступу Компании в среды разработки, тестирования и продуктивную среду Продукта в инфраструктуре YADRO:

a. Сотрудники Компании не могут иметь доступа к любым сетям, средам, интегрируемым системам, в которых содержатся продуктивные данные.

b. Для разбора ошибок, возникающих в продуктивных средах и интегрируемых системах, YADRO передает Компании журналы/логи указанных систем.

c. В случае необходимости использования в средах разработки и тестирования персональных данных, Компания должна предоставить YADRO инструкцию по обезличиванию персональных данных, которые могут обрабатываться в Продукте.

d. Доступ сотрудникам Компании к средам разработки и тестирования предоставляется на основе учетной записи в Active Directory YADRO. Такая учетная запись выдается сотруднику Компании на основании запроса сотрудника владельца соответствующей среды. Выданная учетная запись предоставляет доступ к средам разработки и тестирования в соответствии с ролью сотрудника Компании.

8. Меры ИБ к цепочке поставок

8.1. Компания обязуется обеспечить соответствие всех участников цепочки поставок (включая подрядчиков и поставщиков), вовлеченных в разработку и поставку ПО, требованиям информационной безопасности, установленным для Компании. Компания несет ответственность за выполнение этих требований всеми участниками цепочки поставок и обязуется принимать меры по контролю и устранению нарушений безопасности, связанных с деятельностью таких участников.

8.2. При обнаружении инцидента информационной безопасности, связанного с цепочкой поставок (supply-chain) (например, компрометация третьих лиц или поставщиков), Компания обязана:

8.2.1. Немедленно уведомить YADRO.

8.2.2. Принять меры по блокировке скомпрометированных каналов или компонентов (за исключением компонентов на основе Open Source, в отношении которых Компания обязуется уведомить YADRO и предоставить рекомендации по минимизации рисков).

8.2.3. Предоставить отчет о причинах инцидента и действиях, предпринятых для его устранения.

8.2.4. Восстановить безопасность цепочки поставок в кратчайшие сроки. В случае использования компонентов с открытым исходным кодом (Open Source) Пользователь обязуется уведомить YADRO и предоставить рекомендации по минимизации рисков в соответствии с возможностями и политиками соответствующих сообществ.

8.3. Все ПО, поставляемое Компанией в рамках каждого релиза, должно быть подписано цифровой подписью, чтобы подтвердить его целостность и аутентичность. Компания обязана предоставить YADRO инструменты для проверки цифровой подписи и целостности поставляемого ПО.

9. Ответственность

9.1. Компания несет ответственность за нарушение настоящих Требований о ИБ и обязана возместить YADRO реальный ущерб, документально подтверждённый и возникший вследствие неисполнения или ненадлежащего исполнения Компанией указанных требований. Возмещение ущерба осуществляется в размере, необходимом для восстановления нарушенных прав YADRO, включая затраты на устранение последствий инцидента и восстановление нарушенной информационной безопасности.

9.2. Компания несет ответственность за нарушение настоящих Требований информационной безопасности, допущенное его сотрудниками или третьими лицами, привлечёнными им для исполнения Договора, и обязан возместить YADRO реальный документально подтверждённый ущерб, возникший вследствие таких нарушений. Возмещение ущерба осуществляется в размере, необходимом для восстановления нарушенных прав YADRO, включая затраты на устранение последствий инцидента и восстановление нарушенной информационной безопасности.

9.3. За каждый выявленный случай нарушения требований информационной безопасности со стороны сотрудников Компании YADRO вправе применить штрафные санкции.

9.3.1. За систематические нарушения (три и более) — право YADRO на расторжение Договора в одностороннем порядке, возмещение убытков и упущенной выгоды в полном объеме.