Утверждено
Приказом АО «РТКомм.РУ»
№ 120-РТК от «28» апреля 2026 г.

СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОДРЯДЧИКОВ ПРИ ВЫПОЛНЕНИИ РАБОТ ДЛЯ АО «РТКомм.РУ»

1.Назначение

Настоящие Стандарты информационной безопасности для подрядчиков при выполнении работ для АО «РТКомм.РУ» (далее - Стандарт) устанавливает требования и рекомендации, предъявляемые АО «РТКомм.РУ» (далее - Компания) к третьим лицам/подрядчикам/поставщикам/другим организации/физическими лицами/лицами, занимающимися предпринимательской деятельностью без образования юридического лица, том числе лиц, привлекаемых поставщиками/подрядчиками/другими организациями/физическими лицами/лицами, занимающимися предпринимательской деятельностью без образования юридического лица, с которыми АО «РТКомм.РУ» вступает в отношения и/или привлекаемых лиц АО «РТКомм.РУ» для оказания услуг/выполнения работ и т.д. (далее каждый и по отдельности – Подрядчик и/или Контрагент) и необходимые для обеспечения информационной безопасности и защиты интересов Компании при использовании Подрядчиками информационных активов Компании и/или прямо и/или косвенно взаимодействующие с информационными активами Компании.

Настоящий Стандарт применим ко всем Подрядчикам и их субподрядчикам, которые хранят, обрабатывают и/или имеют доступ к данным Компании. Требования настоящего Стандарта в обязательном порядке включаются в договоры с Подрядчиками, которые хранят, обрабатывают и/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.

Настоящий Стандарт включает в себя как сам текст Стандарт, так и приложения к нему, которые могут трактоваться как самостоятельно каждый из приложений, либо же как целый единый документ. При этом не зависимо от восприятия и применения частей Стандарта, применяется в целом (включая все приложения) как единый документ для исполнения Подрядчиками.

В контексте настоящего Стандарта термин «Информация» включает как Конфиденциальную информацию, так и Персональные данные, используемые в процессе осуществления коммерческой деятельности, в том числе и любую иную информацию, которую Компания согласно внутренним нормативным документам и/или в силу действующего законодательства РФ, относится к информации ограниченного пользования, не предназначенного для распространения/опубликования/передачи третьим лицам (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 и/или служебную информацию, определение которой приведено в Соглашение о конфиденциальности между Подрядчиком и Компанией и/или информацию, доступ, к которой Подрядчик получает, исполняя свои обязательства по любому договору заключенному с Компанией. Далее по тексту термин «Информация» может включать более широкое токование, нежели изложено в настоящем абзаце Стандарта и/или термин «Информация» может включаться в иные термины в целях все объемлемого восприятия применяемой терминологии в настоящем Стандарте.

Настоящим поясняется, что настоящий 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 электронных вычислительных машинах (ЭВМ) и на электронных устройствах (включая предоставленные компанией устройства и устройства, используемые в рамках исполнененнием Подрядчиком своих обязанностей по заключенному договору/договорах с Компанией;
- версии такой Информации на неэлектронных носителях
- и так далее.

Компания оставляет за собой право проводить аудит Подрядчиков и их субподрядчиков, если они не предоставляют гарантий соответствия требованиям, установленных настоящим Стандартом на ежегодной основе и/или в связи выявлением инцидентов и/или отступлений Подрядчика от настоящих Стандартов, или за исключением 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 (десять) рабочих дней.

Компания в праве применять иные меры контроля, не противоречащие действующему законодательству РФ.

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). Условия наступления событий могут быть расширены ниже по тексту и/или конкретизированы под индивидуальные особенности.

Критерии проведения аудита включают соблюдение Подрядчиком требований контроля и положений, указаны в настоящем Стандарте. Критерии могут быть расширены Компаний в одностороннем порядке, а Подрядчик не вправе ссылаться на не указание Компанией первоначально таким критериям, если такие критерии были дополнительно направлены Компанией Подрядчику, в том числе включены в последующие редакции настоящих Стандартов.

2. **Термины, определения и сокращения**

2.1. Информационный актив (для целей Стандарта) – учетная единица, представляющая собой:

- информационную систему;
- информационно-телекоммуникационную сеть и сеть связи, включая их компоненты и/или отдельные части;
- автоматизированную систему управления;
- инфраструктуру центра обработки данных или облачную инфраструктуру,

а также совокупность таких учетных единиц, и задействованная при реализации бизнес-процессов владельца Информационного актива и (или) в отношении которой законодательством Российской Федерации или внутренними документами Владельца Информационного актива установлены требования к обеспечению свойств безопасности информации.

Понятие «Информационный актив» включает в себя также термин «Информацию» и любую иную информацию, обрабатываемую и/или подлежащую обработке в таком информационном активе.

2.2. Владелец Информационного актива (для целей Стандарта) – лицо, которое уполномочено распоряжаться, организовывать и координировать по отношению к Информационному активу процессы учета и категорирования, управления развитием, обслуживанием, использованием, обеспечением безопасности.

2.3. Государственный заказчик (для целей Стандарта) – государственный орган, государственное унитарное предприятие, государственное учреждение, выступающее в роли Владельца Информационного актива и/или заказчика работ / услуг по заключенному с

АО «РТКомм.РУ» контракту.

2.4. Инцидент информационной безопасности – появление одного или нескольких нежелательных и/или непредвиденных событий информационной безопасности, с которыми связана вероятность компрометации бизнес-операций и/или создания угрозы информационной безопасности или нарушения требований законодательства Российской Федерации по защите информации, а также требований настоящего Стандарта.

2.5. Представитель Подрядчика (далее так же «Представитель Контрагента» или «Представитель») – работник Контрагента, принимающий участие в выполнении работ / оказании услуг по Договору, или иное лицо, уполномоченное Подрядчиком для выполнения работ / оказании услуг по Договору.

2.6. Договор – любой гражданско-правовой договор, заключенный между Подрядчиком и Компаний.

Настоящий перечень терминов, определений и сокращений не является исчерпывающим.

3. Обязательства и заверения

3.1. Подрядчик обязуется соблюдать требования по информационной безопасности, предусмотренные законодательством Российской Федерации, договором, заключенным между Компаний и Подрядчиком, настоящий Стандарт, а также проводить мероприятия по информационной безопасности, указанные внестоящих Стандартах.

3.2. В случае привлечения Подрядчиком для исполнения Договора третьих лиц, Подрядчик обязан обеспечить выполнение такими третьими лицами условий настоящего Стандарта, в том числе посредством включения аналогичных условий в договоры с такими третьими лицами и обеспечением контроля их выполнения.

3.3. Настоящий Стандарт информационной безопасности применяется ко всем субподрядчикам, используемым Подрядчиком, которые работают с Информацией и/или Информационными активами, 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 и его соблюдение таким субподрядчиком, в том числе получить согласно разделу 4 настоящего Стандарта Обязательство. 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 и так далее

3.4. Работники Подрядчика, как и работники субподрядчиком, привлекаемые для исполнения Договора должны пройти соответствующее обучение по программе в области обеспечения информационной безопасности, включая требования к защите и безопасной работе с Информацией/Информационным активом. Материалы программы обучения должны периодически пересматриваться и обновляться. Обучение производиться в специализированных учебных заведениях, имеющих право проводить соответствующее обучение, либо же на обучение проводиться на основании материалов, разработанных специализированной организаций. По запросу необходимо предоставлять краткий обзор завершенного обучения.

3.5. 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. Настоящее правило распространяются и на привлекаемых к исполненную Договора субподрядчиков.

3.6. 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 (по согласованию с представителем Компании заверенные копии) этих обязательств Компании в течение 14 (четырнадцати) календарных дней после подписания путем направления заказным письмом с

уведомлением о вручении или передачи уполномоченному работнику Компании.

3.7. 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.

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

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

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

3.11. Подрядчик должен информировать Компанию и получать письменное одобрение перед использованием услуг субподрядчиков, которые либо намереваются работать с Информацией и/или Информационным активом, либо будут иметь доступ к системам Подрядчика или Компании, в которых находятся Информация и/или Информационный актив, а также уведомлять Компанию о том, в какой стране(-ах) будет осуществляться работа с Информацией и/или Информационным активом.

4. Общие требования по информационной безопасности

4.1. Стороны обязуются соблюдать требования о конфиденциальности информации, предусмотренные любым договором, заключенным между Подрядчиком и Компанией.

4.2. Подрядчик имеет право предоставлять доступ к создаваемым и используемым в рамках исполнения Договора материалам только лицам, непосредственно задействованным в выполнении работ и/или оказании услуг по Договору, в объеме, необходимом для выполнения работ / оказания услуг по Договору.

4.3. Подрядчик гарантирует, что его действия (бездействие) не приведут к появлению скрытых функциональных возможностей (недокументированных изменений, операций, либо внедренных «программных закладок»), а также компьютерных вирусов, троянов, самоликвидирующихся механизмов, механизмов защиты от копирования и других подобных машинных команд, которые могут деактивировать, уничтожить или иным образом изменить данные Компании и/или иного Владельца Информационного актива, программное или аппаратное обеспечение Компании и/или иного Владельца Информационного актива.

4.4. Подрядчик обязуется принять все необходимые и достаточные меры по предотвращению деструктивных воздействий (в т.ч. модификация, искажение, удаление) и несанкционированному доступу к Информационным активам Компании и/или иного Владельца Информационного актива и информации, обрабатываемой в таких Информационных активах.

4.5. Подрядчик обеспечивает принятие внутренних документов в области информационной безопасности и гарантирует их наличие, включая, но не ограничиваясь:

- политика информационной безопасности;
- планы реагирования на компьютерные инциденты;
- регламенты действий персонала в случае нештатных ситуаций;
- иные документы, регламентирующие информационную безопасность.

Заказчик вправе запросить, а Подрядчик обязан предоставить указанные в настоящем пункте Стандарта документы в течения срока действия Договора.

4.6. Подрядчик обязан обеспечить проведение внешнего аудита информационной безопасности не реже чем 1 раз в 2 года. Результаты проведенных внешних аудитов информационной

безопасности предоставляются Подрядчиком Компании по его запросу.

4.7. Подрядчик обязуется 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.

Контрагент обязан предоставить информацию обо всех подрядных организациях, которые имеют доступ в информационную инфраструктуру Подрядчика. Такой перечень с указанием наименования Подрядчика, наименований и ИНН подрядных организаций Подрядчика должен быть направлен в Компанию на электронную почту по адресу access@rtcomm.ru с темой письма «Учет подрядных организаций контрагента/подрядчика» не позднее чем через 14 (четырнадцать) календарных дней с момента заключения Договора и затем по мере изменения списка актуальных подрядных организаций Контрагента, но не реже чем 1 раз в полгода.

4.8. В рамках исполнения обязательств по Договору Компания вправе запрашивать информацию и документы, подтверждающие соблюдение Подрядчиком условий настоящего Стандарта, а также осуществлять очную верификацию предоставленной информации. Подрядчик при получении запроса обязуется не позднее 14 (четырнадцати) дней с момента получения запроса представить запрошенную информацию и подтверждающие её документы, в том числе посредством заполнения опросных листов, и обеспечить содействие представителям Компании в случае проведения очной верификации предоставленной информации.

4.9. Компания вправе инициировать проведение совместных с Подрядчиком мероприятий по тестированию планов реагирования и восстановления в случае возникновения нештатных ситуаций или инцидентов информационной безопасности путем имитации указанных событий (проведение тренировок). Порядок и условия проведения указанных мероприятий согласовываются Сторонами дополнительно. При этом предельный срок согласования не должен превышать 10 (десять) календарных дней с даты получения запроса Подрядчиком от Компании соответствующего запроса о проведении проверки.

4.10. В случае предоставления доступа к Информационным активам /информационной инфраструктуре Компании Подрядчик обязуется ознакомить своих Представителей, с условиями настоящего Стандарта и обеспечить получение от них Обязательство о соблюдении настоящего Стандарта по форме, приведенной в Приложении № 1 к настоящему Стандарту. Подрядчик обязуется обеспечить хранение Обязательств, полученных в соответствии с настоящим пунктом Стандарта, в течение срока действия Договора и не менее 3 (трёх) лет после его окончания. В случае получения запроса со стороны Компании, Подрядчик обязан предоставить подтверждение наличия Обязательств о соблюдении настоящего Стандарта от всех своих Представителей.

4.11. Компания вправе ограничить Подрядчику доступ к Информационным активам Компании и/или иного Владельца Информационного актива в случае нарушения Подрядчиком требований по информационной безопасности, предусмотренных законодательством Российской Федерации, Договором и условиями настоящего Стандарта, в том числе иными требованиями, предъявляемыми Компанией в рамках исполнения Подрядчиком Договора. При выявлении указанных нарушений со стороны Подрядчика Компания направляет Подрядчику соответствующее уведомление с указанием сроков устранения нарушения. Подрядчик обязан устранить выявленные нарушения в указанные в уведомлении сроки. В случае несоблюдения срока устранения нарушений, указанного в уведомлении, доступ Подрядчика к Информационным активам Компании и/или иного Владельца Информационного актива может быть ограничен. В этом случае период, на который Подрядчик отстраняется от исполнения обязательств, не может считаться периодом просрочки исполнения обязательств Компании по любому из обязательств по любому из Договоров. Оплата работ /услуг и/или компенсация затрат Подрядчика, понесенных в период ограничения доступа Подрядчика к Информационным активам Компании и/или иного Владельца Информационного актива, не производится.

4.12. Подрядчик должен проводить непрерывную оценку уязвимостей и своевременно исправлять проблемы, связанные с приложениями, операционными системами и прочими компонентами

инфраструктуры. В дополнение Подрядчик обязуется 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.

4.13. Подрядчик должен применять следующие меры контроля:

a. Ежегодные независимые проверки на проникновение в их сети и приложения, отвечающие за обработку Информации или отвечающие за доступ к Информационным активам.

b. Необходимо проводить ежеквартальный поиск уязвимостей в системе безопасности своих платформ и сетей, которые обрабатывают Информацию или которые подключаются к Информационным активам, 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 нормативноправового соответствия.

d. При необходимости Подрядчик обеспечит Компании возможность проведения теста защиты информационных систем от несанкционированного доступа.

5. Взаимодействие при возникновении инцидентов информационной безопасности

5.1. Подрядчик обязан безотлагательно предпринимать все необходимые меры по предотвращению и минимизации ущерба Компании и/или иного Владельца Информационного актива при возникновении инцидентов информационной безопасности.

5.2. При возникновении в инфраструктуре Подрядчика инцидента информационной безопасности, последствия которого могут затронуть интересы Компании (в том числе клиентов или партнеров Компании) и/или иного Владельца Информационного актива, Подрядчик обязан незамедлительно известить об этом Компанию, но не позднее 3-х (трех) часов с момента обнаружения такого инцидента (подозрения на инцидент). При этом Компания оставляет за собой право:

- разорвать любые сетевые связности между своими сетями и сетями Подрядчика;
- заблокировать или отозвать учетные записи и доступа к ресурсам Компании и/или иного Владельца Информационного актива, предоставленные Подрядчику.

5.3. Извещение необходимо для инцидентов информационной безопасности, удовлетворяющий хотя бы одному из следующих критериев:

- невозможность выполнения бизнес-операций или ограничение функциональности Информационного актива;
- разглашение аутентификационных данных или конфиденциальной информации, в том числе персональных данных;
- воздействие вредоносного программного обеспечения;
- массовые блокировки учетных записей, создание несанкционированных учетных записей;
- выявленные признаки несанкционированного доступа или неудачных попыток получения несанкционированного доступа, а также злоупотребление привилегиями;
- нарушение правил и/или требований по информационной безопасности;
- нарушение правил и/или требований по организации удаленного доступа к информационным активам;
- выявленные компьютерные атаки на ресурсы, принадлежащем любой из Сторон и/или Владельцу Информационного актива;
- DDOS-атака на Информационные активы Сторон и/или иного Владельца Информационного актива – выявленная, закончившаяся или планируемая.

5.4. В целях оперативного взаимодействия Стороны назначают лиц, ответственных за обмен информацией об инцидентах (подозрениях на инциденты) информационной безопасности:

от Компании	от Подрядчика
Группа по информационной безопасности Службы безопасности электронная почта: access@rtcomm.ru телефон: +7 (495) 988-77-78, доб. 6614 / 6331/ 6429 / 6429	*Подрядчик обязан направить в течении одного дня с даты заключения Договора информацию Компании о назначенном со стороны Подрядчика ответственного, в том числе подразделение и контактную информацию. Информация, указанная в настоящем пункте, предоставляется письмом на официальном бланке за подписью единоличного исполнительного органа Подрядчика*

5.5. В случае устранения инцидента информационной безопасности Подрядчик обязан уведомить Компанию о мерах, предпринятых для локализации и устранения инцидента в течение 24 (двадцати четырех) часов после его устранения.

5.6. Стороны договариваются обмениваться информацией об инцидентах в свободном формате. Для повышения оперативности при передаче технической информации Стороны вправе использовать телефонную связь, электронную почту и иные каналы передачи информации.

5.7. Подрядчик в целях исполнения Стандарта и Договора 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).

6. Заключительные положения

6.1. Условия настоящего Стандарта являются обязательными для исполнения любой из перечисленных в настоящем Стандарте Сторон и распространяются на отношения Сторон, связанные с исполнением обязательств по Договору.

6.2. Стандарт является неотъемлемой частью Договора и действует до исполнения всех обязательств по Договору, включая срок, прямо указанный в настоящем Стандарте.

6.3. Подрядчик несет ответственность в соответствии с законодательством Российской Федерации за нарушение условий настоящего Стандарта, включая необеспечение конфиденциальности информации и несоблюдение условий ее обработки, и обязан возместить Компании причиненные убытки, возникшие по причине несоблюдения условий настоящего Стандарта и Договора.

6.4. В случае нарушения условий настоящего Стандарта Компания вправе отказаться от Договора полностью или в части без компенсации Подрядчику понесенных убытков.

6.5. Любые Приложения к настоящему Стандарту обязательны для применения Подрядчиком (в том числе и привлекаемыми Подрядчиком субподрядчиками) без каких-либо изъятий, оговорок и ограничений. Приложения к настоящему Стандарту могут содержать конкретизацию каких-либо требований, при этом в случае, если какое-либо требование в Приложении противоречит изложенному в самом Стандарте приоритет имеет требование, изложенное в Приложении.

6.6. Признание какого-либо из требований, обязательств Подрядчика в судебном порядке как в самом Стандарте, так и в приложении не действительным не отменяет требования не иных требований и обязательств, изложенных в самом Стандарте или Приложении к нему.

7. Перечень приложений к Стандарту

7.1. Приложение № 1. Форма обязательства о соблюдении требований информационной

безопасности.

7.2. Приложение № 2. Требования информационной безопасности при предоставлении удаленного доступа к информационным активам.

7.3. Приложение № 3. Требования по информационной безопасности при разработке программного обеспечения.

7.4. Приложение № 4. Требования информационной безопасности при внедрении/модернизации и/или сопровождении информационных активов.

7.5. Приложение № 5. Требования информационной безопасности при предоставлении доступа к объектам критической инфраструктуры.

7.6. Приложение № 6. Порядок обеспечения информационной безопасности при выполнении работ / оказании услуг по созданию и/или эксплуатации государственной информационной системы.

7.7. Приложение № 7. Требования информационной безопасности для партнеров, осуществляющих размещение и обработку информации в целях продвижения услуг и продуктов Компании.

Приложение № 1
к Стандартам информационной безопасности
для подрядчиков при выполнении
работ для АО «РТКомм.РУ»

Форма
Обязательства о соблюдении требований информационной безопасности

Начало формы

ОБЯЗАТЕЛЬСТВО О СОБЛЮДЕНИИ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Я, _____, являясь Представителем _____ (далее – «**Исполнитель**»), обязуюсь выполнять перечисленные ниже требования: Предоставленный мне доступ к Информационным активам/информационной инфраструктуре АО «РТКомм.РУ» и(или) третьих лиц, включая автоматизированные системы (ИС), оборудование, автоматизированных рабочие места, серверы, средства вычислительной техники (СВТ), использовать исключительно в целях исполнения обязательств по заключенным Исполнителем с АО «РТКомм.РУ» договорам. работ на средствах вычислительной техники:

2.1. Оставляя рабочее место, блокировать сеансы доступа к ИС, оборудованию, СВТ.

2.2. Не прерывать сканирование антивирусным ПО съемных машинных носителей информации (USB-носителей, оптических дисков, внешних жестких дисков и др.) при их подключении к автоматизированному рабочему месту (АРМ), СВТ и компонентам ИС.

2.3. Соблюдать парольную политику в части удовлетворения следующим требованиям:

– при работе с паролями запрещается:

- сообщать свой пароль кому-либо;
- пересылать пароли в открытом виде по любым каналам связи;
- пересылать пароли от зашифрованных архивов вместе с такими архивами;
- использовать чужие учетные записи и пароли для коллективного доступа к ИС и технологическим системам;
- использовать один и тот же пароль для разных учетных записей или в разных ИС (за исключением ИС, которые используют единую доменную авторизацию);
- хранить пароли на компьютерах и других средствах хранения информации в незашифрованном виде, на бумаге или других носителях, где неуполномоченные лица могут получить к ним доступ;
- хранить пароли в онлайн сервисах хранения паролей;
- осуществлять ввод пароля на недоверенных компьютерах (например, компьютер в гостинице, чужой телефон или ноутбук).

– длина пароля должна быть не менее 12 символов;

– пароль должен содержать в себе символы как минимум трех категорий из четырех: буквы нижнего регистра (от a до z), буквы верхнего регистра (от A до Z), цифры (от 0 до 9) и спецсимволы (например: $, #, %);

– пароль не должен совпадать с логином и повторять предыдущие 12 паролей для данной учетной записи пользователя;

– пароль, используемый работником для удаленного доступа к Информационным активам АО «РТКомм.РУ», не должен совпадать с какими-либо другими паролями работника;

– пароль не должен включать осмысленные слова, словосочетания, общепринятые аббревиатуры, а также основываться на доступных данных о пользователе (фамилии, дате рождения, именах родственников, номеров телефонов и др.) или легко угадываемом алгоритме смены;

– пароль не должен содержать широко известные или легко угадываемые слова и последовательности символов (12345678, password, qwerty, aaabbb и подобных)

– пароль по умолчанию (созданный при создании учетной записи пользователя) должен быть изменен пользователем при первом входе в систему;

– пароль должен изменяться не реже чем 1 раз в 90 дней с момента последнего изменения;

– в случае разглашения или компрометации пароль должен быть незамедлительно изменен.

2.4. Соблюдать следующие правила обращения с паролями:

– не записывать пароль на предметах и материальных носителях, а также не хранить его в файле в открытом виде;

– не использовать один и тот же пароль для различных учетных записей;

– не передавать кому-либо (в т.ч. своим коллегам и руководителям, а также работникам АО «РТКомм.РУ») свой пароль, равно как и использовать чужие пароли при работ на средствах вычислительной техники;

– не осуществлять попытки подбора паролей (в том числе автоматизированными способами), не пытаться завладеть паролями других лиц.

2.5. Не организовывать на предоставленных АО «РТКомм.РУ» СВТ 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 иные схожие по своим последствиям действия).

2.6. Не предпринимать попытки преодоления установленных АО «РТКомм.РУ» ограничений, отключать и/или удалять установленные на предоставленных АО «РТКомм.РУ» СВТ средства защиты информации (в том числе антивирусное программное обеспечение), использовать недокументированные свойства, ошибки в программном обеспечении (ПО) и настройках доступа к информационным ресурсам АО «РТКомм.РУ», доступ к которым не был предоставлен явным образом.

2.7. Не устанавливать на предоставленные СВТ АО «РТКомм.РУ» какое-либо программное обеспечение кроме ПО, предусмотренного к установке по условиям Договора, изменять настройки уже имеющегося ПО. По вопросам установки необходимого ПО, а также получения административных прав в операционных системах средств вычислительной техники обращаться к ответственному лицу АО «РТКомм.РУ».

2.8. Не хранить и не использовать на предоставленных средствах вычислительной техники программное обеспечение и другие результаты интеллектуальной деятельности в нарушение прав их законных правообладателей.

2.9. В случае предоставления СВТ, не вскрывать корпус предоставленного средства вычислительной техники АО «РТКомм.РУ» (в том числе для самостоятельного устранения неисправностей), самовольно подключать к нему какое-либо оборудование (GPRS модемы, Wi-Fi точки доступа и пр.).

2.10. Не подключать к предоставленным средствам вычислительной техники АО «РТКомм.РУ» личные мобильные устройства (телефоны, смартфоны, планшетные компьютеры, ноутбуки), беспроводные (радио) интерфейсы, модемы и прочее оборудование, позволяющее выходить в сеть Интернет и другие публичные сети.

3. Не использовать ПО следующих категорий при подключении к сети АО «РТКомм.РУ» и работе внутри инфраструктуры АО «РТКомм.РУ» (за исключением случаев прямо предусмотренными условиями Договора):

– сканеры портов и анализаторы трафика;

– средства для организации удаленного доступа, не предусмотренные Договором, включая средства для создания зашифрованных каналов связи (VPN-, DNS-, SSH-, HTTPS-туннели и пр.);

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

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

– ПО, предназначенное для сокрытия или внедрения дополнительной информации в цифровые объекты (в том числе реализующее методы стеганографии);

– ПО, осуществляющее сбор информации с клавиатуры, экрана, микрофона (снифферы);

– специализированные программные средства, оказывающее влияние на сетевые настройки средств вычислительной техники, серверов и сетевого оборудования.

4. Не оставлять без присмотра или передавать кому-либо предоставленные идентификаторы и прочие средства идентификации.

5. По требованию уполномоченных представителей АО «РТКомм.РУ» предоставлять выданные средства вычислительной техники АО «РТКомм.РУ» и носители информации (USB-Flash, CD/DVD и др.) для проверки выполнения требований информационной безопасности.

6. Информировать ответственное лицо АО «РТКомм.РУ» по вопросам защиты информации обо всех инцидентах безопасности информации и событиях, создающих угрозу причинения ущерба АО «РТКомм.РУ», а также об обращениях третьих лиц с целью незаконного получения конфиденциальной информации АО «РТКомм.РУ».

7. При предоставлении доступа к объектам критической инфраструктуры Российской Федерации (далее – ОКИИ), а также информации ограниченного доступа об объектах критической информационной инфраструктуры (далее – ИОД ОКИИ) одного или нескольких видов, включенных в Стандарты информационной безопасности для подрядчиков при выполнении работ для АО «РТКомм.РУ» и Приложения к нему, не совершать следующих действий:

– разглашать ИОД ОКИИ и использовать эту информацию в личных целях (статьях, выступлениях и пр.);

– предоставлять доступ к ИОД ОКИИ третьим лицам;

– копировать, записывать, печатать, принимать, передавать, предоставлять, размножать, уничтожать, обрабатывать, перемещать ИОД ОКИИ, за исключением случаев, предусмотренных Договором;

– размещать (копировать) ИОД ОКИИ на внешние информационные ресурсы, в том числе размещенные в сети Интернет, за исключением случаев, предусмотренных Договором;

– использовать ИОД ОКИИ в открытой переписке по незащищенным каналам связи;

– снимать копии с документов и других носителей ИОД ОКИИ и/или делать выписки из них, а равно использовать различные технические средства (фотоаппараты, видео и звукозаписывающую и иную аппаратуру) для записи ИОД ОКИИ, за исключением случаев, предусмотренных Договором.

Я подтверждаю, что ознакомлен(-а) с Стандартами информационной безопасности для подрядчиков при выполнении работ для АО «РТКомм.РУ», включая Приложения к нему и условия настоящего Обязательства о соблюдении требований информационной безопасности.

Я предупрежден(а) о том, что, АО «РТКомм.РУ» вправе контролировать мои действия при работе с Информационными активами АО «РТКомм.РУ», включая анализ отправленных мной информационных сообщений.

Я предупрежден(а) о том, что АО «РТКомм.РУ» вправе использовать полученную в результате такого анализа информацию для проведения расследований, в том числе, с привлечением правоохранительных органов, а также использовать в качестве доказательств в суде, и подтверждаю, что в этих случаях я не вправе рассчитывать на соблюдение в отношении этих сообщений конфиденциальности со стороны АО «РТКомм.РУ».

«___» _____ 20___ _____/_____

(подпись)/(ФИО)

Приложение № 2
к Стандартам информационной безопасности
для подрядчиков при выполнении
работ для АО «РТКомм.РУ»

Требования информационной безопасности при предоставлении удаленного доступа к Информационным активам

1. Подрядчику предоставляется удаленный доступ к информационным активам Компании. Конкретизированные наименования Информационных активов Компании, к которому предоставляется доступ Подрядчику указывается в заключенном Договоре. Настоящие правила и обязанности едины при предоставлении доступа к любым Информационным активам Компании Подрядчикам Компанией.

2. Удаленный доступ к Информационным активам Компании предоставляется Подрядчику исключительно в целях исполнения Договора и в течение срока действия Договора. После истечения срока действия Договора или его досрочного расторжения доступ прекращается.

3. Удаленный доступ к Информационным активам Компании, содержащим персональные данные, предоставляется только при соблюдении требований действующего законодательства Российской Федерации в области обработки и защиты персональных данных, а также соответствующих условий Договора.

4. Удаленный доступ к Информационным активам государственного заказчика, реализуемый при выполнении работ / оказании услуг по созданию и/или эксплуатации государственной информационной системы, предоставляется в соответствии с порядком, определяемым государственным заказчиком.

5. Для взаимодействия с Компании по организации удаленного доступа к Информационным активам Компании и контроля соблюдения требований по их использованию Подрядчик определяет своих Представителей, и направляет сведения о них Компании в течение 3 (трех) рабочих дней с даты подписания Договора. В случае изменения состава Представителей, Подрядчик обязан уведомить о данном факте и направить сведения о новых Представителях в Компании не позднее 5 (пяти) рабочих дней до момента такого изменения.

6. В случае привлечения Подрядчиком к исполнению обязательств по Договору третьих лиц в соответствии с условиями, определенными в Договоре, таким третьим лицам может быть предоставлен удаленный доступ к Информационным активам Компании, указанным в п. 1 настоящих Требований, при условии подписания отдельного Соглашения о соблюдении такой третьей стороной настоящих Требований, в том числе посредством включения аналогичных условий в договоры с третьими лицами и контроля их выполнения.

7. Удаленный доступ к Информационным активам Компании предоставляется Подрядчику на основании направляемой Подрядчиком информации:

– наименование Информационного актива,

– необходимые права на доступ,

– фамилия, имя, отчество Представителя Подрядчика, его контактный телефон и адрес электронной почты.

В случае привлечения Подрядчиком иностранных граждан или лиц без гражданства, указать для них: фамилия, имя (буквами русского алфавита и буквами латинского алфавита), отчество (при наличии) (буквами русского алфавита), дата рождения (день, месяц, год), пол, гражданство (подданство) иных государств (при наличии), место рождения (государство, населенный пункт), место постоянного проживания (государство, населенный пункт), документ, удостоверяющий личность (серия, номер, дата выдачи, кем выдан), идентификационный номер налогоплательщика или аналогичный документ, используемый в иностранном государстве.

8. На основании информации, предоставленной Подрядчиком, создается учетная запись. Подрядчик несет ответственность за актуальность и достоверность представленной информации.

9. Удаленный доступ к Информационным активам Компании и/или государственного заказчика предоставляется минимально необходимый для исполнения Подрядчиком обязанностей по Договору или контракту.

10. Компания оставляет за собой право осуществления блокировки неиспользуемых

учетных записей Подрядчиком.

11. В целях своевременного ограничения доступа к Информационным активам Компании Подрядчик обязан информировать Компанию о прекращении статуса своих Представителей (в т.ч. об увольнении работников) не позднее дня прекращения статуса с указанием фактической даты прекращения работ по Договору.

12. Компания определяет VPN-решение (производителя, версии, настроек VPN-клиента), используемое для организации удаленного доступа к Информационным активам Компании.

13. Для удаленного доступа к Информационным активам Компании и/или государственного заказчика Подрядчик обязан использовать только программное обеспечение для удаленного подключения (VPN-решение), определяемое Компанией и/или государственным заказчиком. Подрядчик не вправе вносить какие-либо изменения в VPN-решение или осуществлять удаленный доступ несогласованным с Компанией способом. Доступ к компонентам Информационных активов Компании и/или государственного заказчика посредством публичных сетей без использования VPN-решения запрещен.

14. Подрядчик обязан осуществлять журналирование (логирование) удаленного доступа к Информационным активам государственного заказчика и по требованию Компании или государственного заказчика, в установленные в таком запросе сроки, предоставлять эту информацию автору запроса.

15. Учетная запись пользователя на рабочем месте Подрядчика, с которого осуществляется удаленный доступ к Информационным активам Компании и/или государственного заказчика, не должна обладать административными правами.

16. Подрядчик должен разработать и внедрить в своей инфраструктуре комплекс организационно-технических мероприятий обеспечения информационной безопасности, включающих в том числе следующие меры:

- выделение в отдельный сетевой сегмент рабочих мест, используемых для удаленного доступа к Информационным активам;
- запрет использования на указанных рабочих местах средств удаленного управления (например, «Team Viewer», «AnyDesk, AmmyAdmin, AeroAdmin»);
- запрет использования личных устройств для удаленного подключения к Информационным активам;
- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрация (журналирование, логирование) событий безопасности (в т.ч. попытки входа (выхода) в систему (из системы), запуск (завершение) загрузки ОС, программ и процессов, попытки доступа субъектов доступа к объектам доступа, попытки изменения привилегий учетных записей и конфигурации параметров безопасности), при этом рекомендуемый срок хранения журналов событий безопасности не менее 1 года;
- антивирусная защита;
- выявление, анализ и устранение уязвимостей;
- своевременная установка обновлений безопасности с целью устранения известных уязвимостей;
- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей;
- обнаружение вторжений;
- защита почтовых сервисов от фишинга.

Приложение № 3
к Стандартам информационной безопасности
для подрядчиков при выполнении
работ для АО «РТКомм.РУ»

Требования по информационной безопасности при разработке программного обеспечения

Настоящие требования по информационной безопасности при разработке программного обеспечения применяются Сторонами в случае оказания услуг/выполнению работ Подрядчиками по разработке программного обеспечения в интересах АО «РТКомм.РУ»

1. **Общие требования по организации процесса разработки программного обеспечения**

1.1. Процесс разработки программного обеспечения (далее – ПО) должен осуществляться с учетом требований документов:

– «Методические рекомендации по организации производственного процесса разработки государственных информационных систем с учетом применения итерационного подхода к разработке», утверждены протоколом Президиума Правительственной комиссии от 28.12.2022 № 60 (если ПО входит в состав государственной информационной системы или предназначено для применения в составе государственных информационных систем);

– ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

– ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»;

– ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования»;

– ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств».

1.2. По запросу Компании Подрядчик должен предоставлять подтверждение выполнения мер по безопасной разработке в отношении ПО в объеме, указанном в запросе.

1.3. При использовании в составе ПО программ, программных комплексов или компонентов, разработанных третьими лицами, условия, на которых передается право на использование (исполнение) этих программ, не должны приводить к возникновению ограничений, препятствующих использованию ПО по его прямому назначению.

1.4. В рамках разработки исходного кода ПО должны быть реализованы следующие меры:

– регистрация событий, связанных с изменением исходного кода ПО;

– права по управлению репозиторием и доступу к исходному коду должны быть доступны только минимально достаточному перечню пользователей;

– периодическая ревизия прав доступа пользователей и блокировка неактивных пользователей.

1.5. Подрядчик должен обеспечить выполнение работ по инструментальному исследованию исходного кода ПО в соответствии со следующими требованиями ГОСТ Р 56939:

– статический анализ исходного кода программы;

– экспертиза исходного кода программы в отношении компонентов, заимствованных у сторонних разработчиков ПО;

– динамический анализ исходного кода программы;

– фаззинг-тестирование.

1.6. Подрядчик проводит анализ защищенности разработанного ПО на предмет наличия уязвимостей в исходном коде ПО и в прикладном ПО, в т.ч. в отношении каждого релиза. К приемке допускается только ПО, в отношении которого проведен анализ защищенности и его результаты показывают отсутствие уязвимостей ПО, в том числе уязвимостей прикладного ПО и исходного кода ПО, либо реализацию набора компенсирующих мер, которые закрывают возможность эксплуатации уязвимостей до момента их полного устранения.

1.7. По запросу Компании Подрядчик должен предоставлять Компании отчетные

документы, содержащие результаты анализа уязвимостей ПО, а также сведения об их устранении.

1.8. Разрабатываемое ПО не должно содержать скрытых функциональных возможностей (в т.ч. недокументированные изменения операций, внедренные «программные закладки»), которые дают неуполномоченным лицам возможность влиять на работу результата работ или получать обрабатываемую и/или хранимую в результате работ информацию.

1.9. . Разрабатываемое ПО не должно содержать компьютерные вирусы, трояны, самоликвидирующиеся механизмы и другие подобные машинные команды, которые могут деактивировать, уничтожить или изменить иным образом данные пользователя, программное или аппаратное обеспечение.

1.10. Для выполнения работ должны использоваться АРМ, в отношении которых должны быть реализованы следующие меры защиты информации:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- антивирусная защита;
- защита мобильных устройств (в случае применения мобильных устройств);
- защита от утечек конфиденциальной информации;
- защита каналов связи и межсетевого взаимодействия.

1.11. Подключение Представителей Подрядчика к инфраструктурным ландшафтам, используемым для разработки ПО, должно осуществляться с использованием средств криптографической защиты информации.

2. **Требования к ограничениям в программном обеспечении**

2.1. Разрабатываемое ПО должно поддерживать операционные системы и СУБД российского производства, сертифицированные по требованиям ФСТЭК России и имеющие поддерживаемые собственные официальные репозитории.

2.2. Общие требования, выполнение которых необходимо учитывать в процессе разработки ПО:

- технологические учетные записи, используемые для обеспечения работы разрабатываемого ПО, должны обладать минимально необходимыми для функционирования полномочиями;
- межсервисные взаимодействия должны проходить обязательные процедуры аутентификации и авторизации;
- разрабатываемое ПО должно использовать единый утвержденный механизм аутентификации, который может быть дополнен включением строгой аутентификации;
- интерфейсы отладки и администрирования в обход штатных механизмов аутентификации должны быть исключены;
- все контроли безопасности (аутентификация, авторизация, валидация и пр.) должны осуществляться на серверной стороне. Не допускается выполнение указанных функций на стороне клиента;
- хранение криптографических ключей и иных секретов (в т.ч. ключи, пароли, токены доступа) в исходном коде, конфигурационных файлах, переменных окружения должно быть исключено. Для хранения секретов должны применяться специализированные решения;
- пароли пользователей должны храниться в БД в хэшированном виде. При этом генерация хэша пароля должна производиться одним из современных алгоритмов, поддерживающих «соль», например, PBKDF2. «Соль» для вычисления хэш-функции должна быть случайной и уникальной для каждого пароля;
- аутентификация сервисов при помощи TLS должна удовлетворять следующим требованиям: взаимная аутентификация обеих сторон взаимодействия; проверка издателя сертификата (удостоверяющего центра); проверка сертификата на валидность (не отозван, не истек срок действия); проверка субъекта сертификата;
- во всех компонентах ПО должны быть удалены или заблокированы все встроенные учетные записи;
- при аутентификации пользователя в приложении каждый раз должен создаваться новый токен, старый при этом должен становиться недействительным;
- хранение сессионных токенов в браузере должно осуществляться в защищенных

файлах cookie или в хранилище сессий HTML5;

– генерация сессионных токенов должна осуществляться надежными криптографическими алгоритмами;

– токены должны обладать конечным сроком действия, при этом по его истечении, а также при выходе из системы токен должен становиться недействительным;

– в приложении должна быть реализована защита от CSRF-атак;

– везде, где это не предусмотрено специально, должен быть отключен просмотр каталогов. Кроме того, приложения не должны разрешать обнаружение или раскрытие метаданных файлов или каталогов, таких как Thumbs.db, .DS_Store, .git или .svn;

– в приложении должны применяться механизмы защиты от атак «загрязнения» параметров HTTP (HTTP parameter pollution);

– все поступающие данные должны проходить форматно-логический контроль по «белому» списку разрешенных типов данных, значений атрибутов, параметров, заголовков, запросов, методов, включая поля HTML-формы, REST-запросы, параметры URL, HTTP-заголовки, атрибуты cookie и т. д.;

– структурированные данные должны быть строго типизированы и проверяться по заданной схеме, в которой указаны разрешенные символы, максимальная длина и шаблон данных;

– при наличии пользовательских визуальных текстовых редакторов весь недоверенный HTML-код должен нейтрализоваться с помощью библиотеки санитизации или средствами html-фреймворка;

– использования eval() или других функций динамического исполнения кода должно быть исключено;

– ПО должно нейтрализовать, удалять или помещать в песочницу предоставляемый пользователем контент на языках сценариев или шаблонов разметки, таких как Markdown, таблицы стилей CSS или XSL, BBCode и т. п.;

– разрабатываемое ПО не должно содержать недокументированной или неиспользуемой функциональности;

– среда разработки и/или тестирования должна быть отделена на логическом или физическом уровне от продуктивной среды;

– в среде разработки и тестирования не допускается использование производственных (продуктивных) данных, включающих защищаемую информацию (за исключением конфигурационной информации, определяющей параметры работы системы);

– разработка и тестирование изменений ПО на продуктивном экземпляре системы не допускается;

– перед вводом ПО в промышленную эксплуатацию должны быть отключены все отладочные функции.

2.3. В ПО должна обеспечиваться регистрация событий безопасности. Состав, содержание и объем событий безопасности определен ГОСТ 59548-2022. Основными категориями действий, для которых требуется регистрация являются:

– аутентификация и авторизация пользователей;

– управление пользователями и конфигурациями;

– управление событиями безопасности в системе.".

2.4. В зависимости от категории действия, должна производиться регистрация следующих основных типов событий:

– успешные/неуспешные аутентификации пользователя в ПО;

– выход пользователя из ПО;

– создание, удаление учетной записи;

– изменение наименования учетной записи;

– изменение пароля учетной записи;

– блокирование (отключение) учетной записи;

– разблокировка(активация) учетной записи;

– назначение, исключение, изменение прав на объект;

– создание, удаление группы (роли) пользователей;

– изменение прав группы (роли) пользователей;

– исключение пользователя из состава группы (роли);

– занесение пользователя в состав группы (роли);
– ошибка обработки запроса пользователя (некорректный запрос);
– очистка журнала аудита;
– отключение журналирования событий информационной безопасности;
– изменение настроек аудита (включение/отключение, изменение уровня логирования);
– успешное/неуспешное изменение конфигурации системы или ее компонентов (конфигурационных файлов, настроек СУБД, настроек ПО)
– включение и отключение компонентов, модулей и служб ПО;
– экспорт и импорт данных;
– создание, удаление, изменение объектов, составляющих ПО;
– запуск (завершение) программ и процессов (заданий, задач).

2.5. Допускается регистрация дополнительных событий безопасности.

2.6. Вне зависимости от категории действия регистрируемые события безопасности должны включать следующую основную информацию:
– название и идентификатор события;
– информацию о выполненной операции (в т.ч. создание, изменение, удаление, просмотр);
– точное время возникновения события;
– информацию об объекте и субъекте операции;
– уникальный идентификатор и имя пользователя в системе;
– уникальный идентификатор сессии пользователя в системе;
– статус выполненной операции (успех/отказ);
– описание причины, в случае неуспешности операции;
– IP адрес и имя источника информации о событии;
– IP адрес и имя хоста, выполнившего операцию;
– IP адрес и имя хоста, на котором зафиксирована операция.

2.7. В зависимости от категории действия, в событии безопасности может быть указана дополнительная информация, в частности:
– информация о user-agent;
– информация о старых и новых значениях измененных свойств;
– название и идентификаторы процессов, служб, файлов и компонентов, участвующих в событии;
– NAT IP адрес хоста, выполнившего операцию.

2.8. Хранение событий безопасности должно быть реализовано одним из следующих способов:
– в формате записей в базе данных,
– в формате текстового файла в одном из структурированных форматов:
а) KeyValue;
б) JSON;
в) XML;
г) CSV (с любым разделителем);
д) CEF;
е) LEEF;
ж) в формате журнала Windows Event Log.

2.9. Срок хранения событий должен составлять не менее 14 дней.

2.10. Разрабатываемое ПО должно иметь возможность передавать события безопасности (предоставлять доступ к ним) как минимум одним из следующих способов:
– отправка событий посредством протокола Syslog;
– выгрузка событий посредством Windows RPC для Windows-ориентированных систем;
– выгрузка событий из базы данных (запрос к базе данных);
– выгрузка событий из текстового файла;
– выгрузка событий через API (REST, SOAP);
– регистрацию событий в программных брокерах сообщений (kafka, rabbit mq).

Приложение № **4**
к Стандартам информационной безопасности
для подрядчиков при выполнении
работ для АО «РТКомм.РУ»

Требования информационной безопасности при внедрении/модернизации или сопровождении Информационных активов АО «РТКомм.РУ»

Настоящие требования информационной безопасности при внедрении/модернизации или сопровождении информационных активов применяются Сторонами в случае оказания услуг/выполненную работ по внедрении/модернизации, сопровождению или эксплуатации информационных активов АО «РТКомм.РУ» со стороны Подрядчика.

1. Подрядчик должен соблюдать требования проектной, рабочей, эксплуатационной документации на Информационный актив (далее – Документация), предоставляемой Подрядчику со стороны Компании.
2. Хранение актуальной Документации, а также иных материалов может быть организовано как в пределах контура Компании, так и на внутренних ресурсах Подрядчика, с соблюдением требований по защите информации. Запрещено размещение Документации и иных материалов на внешних общедоступных ресурсах без соблюдения требований по защите информации.
3. Настройка, обновление версий компонентов Информационного актива должны соответствовать требованиям, указанными в Документации. Проводимые работы не должны приводить к ухудшению защищенности Информационных активов Компании.
4. Изменения компонентов Информационных активов не должно приводить к возникновению новых угроз безопасности информации и существенным изменениям в части состава и категорий обрабатываемой информации, структурно-функциональных характеристик системы, применяемых технологий. Подрядчиком должно осуществляться предварительное тестирование обновлений программного обеспечения. Тестирование обновлений ПО в продуктивном сегменте системы запрещается. Применение не проверенных и заведомо уязвимых компонентов ПО в эксплуатируемом Информационном активе не допускается.
5. Обновление программного обеспечения должно проводиться в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30 июня 2025 г.
6. Для хранения эталонных образов программного обеспечения компонентов, его обновлений и дополнений необходимо использовать доверенные репозитории, указанные в рабочей документации на систему. Подключение к системе сторонних репозиториев, а также публикация в них образов либо исходных кодов программного обеспечения эксплуатируемой системы не допускается.

Приложение № 5
к Стандартам информационной безопасности
для подрядчиков при выполнении
работ для АО «РТКомм.РУ»

Требования информационной безопасности при предоставлении доступа к объектам критической инфраструктуры

Настоящие требования информационной безопасности при предоставлении доступа к объектам критической инфраструктуры применяются Сторонами в случае оказания услуг/выполнению работ, предусматривающих доступ к объектам критической информационной инфраструктуры (КИИ) со стороны Подрядчика.

1. Контрагент в отношении критической информационной инфраструктуры Информационного актива (информационной системы, информационно-телекоммуникационной сети, автоматизированной системы управления, составляющими предмет Договора или, в соответствии с Договором, с которыми подразумевается предоставление доступа) и/или его (её, их) составными частями, являющимся (-щейся, -щимися) объектами критической информационной инфраструктуры Российской Федерации (далее – ОКИИ) и принадлежащими Компании, а также информации ограниченного доступа об объектах критической информационной инфраструктуры (далее - ИОД ОКИИ) в соответствии с указанным ниже перечнем ИОД ОКИИ, обязуется обеспечивать выполнение требований законодательства Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры (далее — КИИ).

№ п/п	Вид информации ограниченного доступа и распространения об объектах критической информационной инфраструктуры
1.	Сведения, принадлежащие к значимому объекту критической информационной инфраструктуры Компании или относящиеся к критической информационной инфраструктуре Российской Федерации, позволяющие в совокупности идентифицировать ОКИИ, в том числе: • наименование ОКИИ; • адрес(а) размещения ОКИИ; • категория значимости; • сведения об ответственных лицах, участвующих в эксплуатации (обеспечении функционирования), а также обеспечении безопасности ОКИИ; • о способах взаимодействия ОКИИ с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводный), протоколов взаимодействия; • сведения о программных и программно-аппаратных средствах, используемых на ОКИИ; • сведения об угрозах безопасности информации и категориях нарушителей в отношении ОКИИ; • возможные последствия в случае возникновения компьютерных инцидентов; • меры, применяемые для обеспечения безопасности ОКИИ.
2.	Совокупность сведений о системе безопасности ОКИИ и средствах защиты информации, применяемых или планируемых к применению: • архитектура системы безопасности ОКИИ; • технические решения системы безопасности ОКИИ, состав средств защиты информации; • сведения об ответственных лицах, участвующих в обеспечении безопасности ОКИИ, в том числе в эксплуатации средств защиты информации.

3.	Электронные закрытые ключи, применяемые для целей шифрования/расшифрования, аутентификации, электронной подписи при реализации процессов управления/администрирования ИТ-инфраструктуры, средств защиты информации в составе объектов КИИ Компании.
4.	Пароли доступа к сетевому оборудованию, удалённому доступу, серверам ИТ-инфраструктуры, средств защиты информации в составе объектов КИИ Компании, а также пароли доступа учётных записей, имеющих администраторские полномочия на аппаратных и программных компонентах ИТ-инфраструктуры, средств защиты информации в составе объектов КИИ Компании.
5.	Настройки (политики) безопасности средств защиты информации и информационных систем, правила межсетевого экранирования и/или правила разграничения доступа коммутационного оборудования (совокупный набор действующих правил межсетевого экрана и/или коммутационного оборудования, включающий адрес источника, адрес назначения, порт, протокол, тип правила), находящегося в составе ОКИИ Компании.
6.	Схемы ЛВС и защиты периметра ИТ-инфраструктуры в составе объектов КИИ Компании с наличием совокупных данных о IP-адресации, типе оборудования и его расположении, схемы информационного взаимодействия, раскрывающие архитектуру ОКИИ и системы безопасности ОКИИ.
7.	Информация об уязвимостях ИТ-инфраструктуры, информационных систем и средств защиты информации в составе объектов КИИ Компании.

2. Контрагенту, имеющему доступ к ОКИИ и/или ИОД ОКИИ, запрещается:

– разглашать ИОД ОКИИ и использовать эту информацию в личных целях (статьях, выступлениях и пр.);

– предоставлять доступ к ИОД ОКИИ третьим лицам;

– копировать, записывать, печатать, принимать, передавать, предоставлять, размножать, уничтожать, обрабатывать, перемещать ИОД ОКИИ, за исключением случаев, предусмотренных Договором;

– размещать (копировать) ИОД ОКИИ на внешние информационные ресурсы, в том числе размещенные в сети Интернет, за исключением случаев, предусмотренных настоящим Договором;

– использовать ИОД ОКИИ в открытой переписке по незащищенным каналам связи;

– снимать копии с документов и других носителей ИОД ОКИИ и/или делать выписки из них, а равно использовать различные технические средства (фотоаппараты, видео и звукозаписывающую и иную аппаратуру) для записи ИОД ОКИИ, за исключением случаев, предусмотренных Договором.

Приложение № 6
к Стандартам информационной безопасности
для подрядчиков при выполнении
работ для АО «РТКомм.РУ»

Порядок обеспечения информационной безопасности при выполнении работ / оказании услуг по созданию и/или эксплуатации государственной информационной системы

Настоящий порядок обеспечения информационной безопасности при выполнении работ / оказании услуг по созданию и эксплуатации государственной информационной системы применяется Сторонами в случае привлечения третьих лиц в рамках государственных контрактов по созданию и/или эксплуатации государственной информационной системы

1.1. Настоящий Порядок обеспечения информационной безопасности при выполнении работ / оказании услуг по созданию и/или эксплуатации государственной информационной системы (далее – «Порядок») определяет условия выполнения работ по созданию и/или эксплуатации государственной информационной системы, конкретизировано указываемый Компаний в Договоре (далее – ГИС) в интересах государственного заказчика, а также требования по обеспечению информационной безопасности при исполнении Подрядчиком условий Договора.

1.2. Подрядчику предоставляется удаленный доступ к ГИС и/или иным Информационным активам государственного заказчика исключительно в целях исполнения Договора и на период срока действия Договора. После истечения срока действия Договора или его досрочного расторжения доступ прекращается.

1.3. Подрядчик обязан:

– соблюдать условия получения удаленного доступа к Информационным активам, предъявляемые государственным заказчиком и условия работы с данными активами, указанные в Порядке;

– не предоставлять третьим лицам доступ к Информационным активам государственного заказчика без предварительного письменного согласия Компании и государственного заказчика;

– обеспечивать конфиденциальность информации, содержащейся в Информационных активах государственного заказчика, не раскрывать и не передавать такую информацию третьим лицам без предварительного письменного согласия Компании и государственного заказчика.

1.4. Подрядчик, получивший доступ к информационным активам государственного заказчика и Компании и (или) содержащейся в них информации для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также для выполнения работ, оказания услуг по защите информации, должен быть ознакомлен с политикой защиты информации государственного заказчика и (или) иными документами, регламентирующими правила и стандарты по защите информации, и исполнять их в части, их касающейся.

1.5. В случае привлечения Подрядчиком к исполнению обязательств по Договору третьих лиц в соответствии с условиями, определенными в Договоре, таким третьим лицам может быть предоставлен удаленный доступ к Информационным активам государственного заказчика при условии соблюдении такой третьей стороной настоящего Порядка, в том числе посредством включения аналогичных условий в договоры с третьими лицами и контроля их выполнения. Подрядчик обязуется обеспечить соблюдение настоящего Порядка третьими лицами, получившими удаленный доступ к Информационным активам государственного заказчика. Компания вправе потребовать от Подрядчика, а Подрядчик обязан обеспечить подписание между Компанией и привлекаемым Подрядчиком третьим лицом отдельного соглашения о соблюдении требований информационной безопасности.

1.6. Автоматизированные рабочие места Подрядчика, используемые для доступа к Информационным активам государственного заказчика, должны соответствовать требованиям о защите информации, установленным в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.7. Для удаленного доступа к Информационным активам государственного заказчика Подрядчик обязан обеспечить нахождение своих Представителей на территории Российской Федерации при выполнении ими работ по Договору или контракту. При использовании Подрядчиком для исполнения обязательств по Договору информационной инфраструктуры, принадлежащей государственному заказчику, Компании или третьим лицам, в том числе в процессе разработки программного обеспечения, запрещается удаленный доступ Представителей Подрядчика к такой инфраструктуре из-за пределов территории Российской Федерации.

1.8. Подрядчик обязан безотлагательно предпринимать все необходимые меры по предотвращению и минимизации ущерба государственному заказчику при возникновении инцидентов информационной безопасности.

1.9. В случаях возникновения угрозы информационной безопасности в отношении Информационных активов государственного заказчика со стороны сети, рабочих мест или иной инфраструктуры Подрядчика, в результате действий Подрядчика, а также претензий со стороны государственных контролирующих и надзорных органов или выявления фактов нарушений, приведших к материальному ущербу, расследование осуществляется Компанией (и/или с привлечением Компанией третьего лица) совместно с Подрядчиком.

1.10. Компания вправе:

– запрашивать информацию, подтверждающую выполнение Контрагентом требований Стандарта и инициировать проверку;

– контролировать действия Подрядчика при предоставлении удаленного доступа к Информационным активам государственного заказчика;

– приостанавливать такой доступ в случаях возникновения ситуаций, создающих угрозу информационной безопасности государственном заказчику, уведомив об этом Подрядчика. Доступ восстанавливается после устранения выявленной угрозы на основании, предоставленной Подрядчиком информации и по согласованию с Компанией и/или государственным заказчиком.

1.11. Подрядчик обязан:

– своевременно предоставлять ответы на запросы со стороны Компании;

– не препятствовать в проведении проверок выполнения Подрядчиком требований Стандарта.

Приложение № 7
к Стандартам информационной безопасности
для подрядчиков при выполнении
работ для АО «РТКомм.РУ»

Требования информационной безопасности для партнеров, осуществляющих размещение и обработку информации в целях продвижения услуг и продуктов АО «РТКомм.РУ»

Настоящие требования информационной безопасности для партнеров, осуществляющих размещение и обработку информации в целях продвижения услуг и продуктов АО «РТКомм.РУ» применяются Сторонами в случае заключения договора с партнерами по осуществлению продвижение услуг и продуктов АО «РТКомм.РУ»

1. Подрядчик должен иметь в штате ответственное лицо за обеспечение информационной безопасности, на которое возложены полномочия по обеспечению информационной безопасности Информационных активов Подрядчика и обрабатываемой Подрядчиком информации.
2. Подрядчик обязуется обеспечить реализацию мер, направленных на безопасность (предотвращение утечек) персональных данных, обрабатываемых и собираемых Подрядчиком в целях исполнения Договора, в том числе посредством Web-сайта, принадлежащего Подрядчику и используемого Подрядчиком для продвижения услуг и продуктов Компании (далее – Web-сайт).
3. Подрядчик обязуется обеспечить размещение Web-сайта и его компонентов (в т.ч. баз данных) и других Информационных активов Подрядчика, посредством которых ведется обработка персональных данных клиентов Компании, на территории Российской Федерации.
4. Подрядчик обязуется иметь и исполнять требования своей внутренней организационно-распорядительной документации, регламентирующей вопросы информационной безопасности, в т.ч:

– обязательное наличие, регулярное обновление и обязательное функционирование средств антивирусной защиты на автоматизированных рабочих местах и серверах;
– требования к порядку и стойкости используемых паролей.

5. Дополнительные требования по защите Web-сайтов.

5.1. Подрядчик обязуется выполнять комплекс организационных и технических мер по информационной безопасности своих Web-сайта, включая следующие:

– обеспечение невозможности использования сайтов Подрядчика в качестве потенциальных фишинговых ресурсов, в т.ч.

- не допускать использования в названии сайтов буквосочетаний «rt», «rtk», «rostelek», «rostelecom», «rtcomm», «sensat» с символами «-», «_» и подобных им;
- не допускать в оформлении сайта цветовых и стилевых решений, позволяющих пользователям сделать предположение о принадлежности сайта Компании;

– защиту Web-сайта от несанкционированного доступа;
– анализ защищенности Web-сайта на наличие уязвимостей;
– закрытие выявленных уязвимостей критического уровня опасности с датой публикации обновлений (компенсирующих мер по устранению) в банке данных угроз ФСТЭК России и (или) на официальных сайтах разработчиков более 30 дней;
– возможность настройки географических ограничений доступа пользователей на Web-сайте.

5.2. Подрядчик обязуется на постоянной основе, но не реже одного раза в год, проводить независимую оценку защищенности Web-сайта методом тестирования на проникновение, и предоставлять его результаты в Компанию по запросу.