СОГЛАШЕНИЕ
о сотрудничестве Национального координационного центра по компьютерным инцидентам и *(наименование контрагента)* в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) в лице директора Скрябина Олега Валерьевича, действующего в соответствии с приказом ФСБ России от 24 июля 2018г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52109), с одной стороны, и *(наименование контрагента)*, (далее – *краткое наименование контрагента*) в лице генерального директора *(ФИО*), действующего на основании *(название документа, подтверждающего полномочия на подписание соглашения)*, с другой стороны, именуемые в дальнейшем Сторонами, согласились о нижеследующем:

Статья 1

1. Для целей настоящего Соглашения используемые понятия означают следующее:

1.1. «Информационные ресурсы» – информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления.

1.2. «Зона ответственности *(наименование контрагента)*» – информационные ресурсы, в отношении которых *(наименование контрагента)* осуществляется деятельность:

а) по обнаружению (выявлению), предупреждению (предотвращению) и ликвидации последствий компьютерных атак, включая:

– выявление признаков компьютерных атак;

– мониторинг информационной безопасности;

– анализ событий информационной безопасности;

– оценку степени защищенности от компьютерных атак, в том числе методом

тестирования на проникновение, и выявление известных уязвимостей программного обеспечения;

– анализ сведений об угрозах информационной безопасности и уязвимостях информационных ресурсов;

– восстановление работоспособности информационных ресурсов (в случае ее нарушения);

– фиксацию следов вредоносного воздействия компьютерной атаки;

– организацию и проведение учений и тренировок, в том числе с использованием специальных учебно-тренировочных центров (киберполигонов);

б) по реагированию на компьютерный инцидент, включая:

– установление причин, условий и канала возникновения компьютерного инцидента, в том числе связи компьютерного инцидента с компьютерной атакой, а также их устранение;

– устранение последствий компьютерного инцидента, а также анализ результатов их устранения.

в) по осуществлению консалтинговых услуг.

1.3. «Консалтинговые услуги» – информационно-консультационные услуги, оказываемые третьим лицам (юридическим лицам и индивидуальным предпринимателям) по направлениям деятельности, предусмотренными подпунктами «а» и «б» пункта 1.2 настоящей статьи.

1.4. «Корпоративный центр обнаружения, предупреждения и ликвидации последствий компьютерных атак» (далее – корпоративный центр) – организационно-техническая структура *(наименование контрагента)*, включающая силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности *(наименование контрагента)*, в том числе в рамках договоров и соглашений с владельцами данных ресурсов.

2. Термины, используемые в Соглашении, понимаются в значениях, определенных Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Национальными стандартами Российской Федерации ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (утвержден и введен в действие приказом Росстандарта от 19 мая 2021 г. № 392-ст) и ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» (утвержден и введен в действие приказом Росстандарта от 29 ноября 2022 г. № 1375-ст).

Статья 2

Предметом настоящего Соглашения является организация взаимодействия при решении Сторонами задач в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты в отношении информационных ресурсов, находящихся в зоне ответственности *(наименование контрагента)*, в рамках государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА).

Статья 3

Головными подразделениями, выполняющими функции по взаимодействию в соответствии с настоящим соглашением, являются:

НКЦКИ;

от *(наименование контрагента)* – корпоративный центр.

Статья 4

1. В рамках настоящего Соглашения Стороны договорились осуществлять взаимодействие по следующим направлениям:

– проведение мероприятий по обнаружению и предупреждению компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности *(наименование контрагента)*;

– проведение мероприятий по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак в отношении информационных ресурсов, находящихся в зоне ответственности *(наименование контрагента)*;

– обмен сведениями о компьютерных атаках и компьютерных инцидентах, связанных с информационными ресурсами, находящимися в зоне ответственности *(наименование контрагента)*;

– отработка механизмов и процедур взаимодействия Сторон при реализации мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности *(наименование контрагента)*;

– проведение совместных тренировок и учений по вопросам функционирования ГосСОПКА;

– повышение уровня осведомленности и квалификации специалистов Сторон в области информационной безопасности;

– совершенствование методической базы, разрабатываемой в целях эффективного функционирования ГосСОПКА;

– проведение совместных семинаров, конференций, выставок и иных мероприятий.

2. Настоящее Соглашение является соглашением о сотрудничестве в значении подпункта «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Статья 5

1. В ходе функционирования корпоративного центра *(наименование контрагента)* осуществляет:

– согласование с НКЦКИ методических документов в части реализации функций обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности *(наименование контрагента)*, в соответствии с рекомендациями НКЦКИ;

– формирование, поддержание в актуальном состоянии и передачу в НКЦКИ сведений об информационных ресурсах, находящихся в зоне ответственности *(наименование контрагента)*, не позднее 5 календарных дней со дня включения в зону ответственности *(наименование контрагента)*, или исключения из зон ответственности *(наименование контрагента)*, информационных ресурсов;

– направление в НКЦКИ информации о компьютерных инцидентах в срок не позднее 3 часов с момента обнаружения компьютерного инцидента, связанного с функционированием значимого объекта критической информационной инфраструктуры Российской Федерации, и не позднее 24 часов с момента обнаружения компьютерного инцидента, связанного с функционированием иных информационных ресурсов;

– выявление в круглосуточном режиме компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности *(наименование контрагента)*, а также протоколирование технической и другой значимой информации об их происхождении и направленности в форме, согласованной Сторонами;

– проведение (в соответствии с методическими рекомендациями НКЦКИ) мероприятий по оценке степени защищенности от компьютерных атак, в том числе методом тестирования на проникновение, информационных ресурсов, находящихся в зоне ответственности *(наименование контрагента)* с предварительным уведомлением НКЦКИ (с использованием личного кабинета корпоративного центра *(наименование контрагента)*, функционирующего в технической инфраструктуре НКЦКИ, электронной почты, а при отсутствии указанных каналов передачи информации – почтовых отправлений) не позднее, чем за 5 рабочих дней до предполагаемого дня их проведения, а также направление в адрес НКЦКИ результатов указанных мероприятий.

В случае, если решение о проведении указанных мероприятий принято менее, чем за 5 рабочих дней до предполагаемого дня их проведения, допускается информировать НКЦКИ в день проведения мероприятий;

– выявление, сбор и анализ сведений об уязвимостях программного обеспечения, используемого на элементах информационных ресурсов, в том числе методом сканирования информационных ресурсов доступных со стороны сети Интернет, находящихся в зоне ответственности *(наименование контрагента)*. Подготовка рекомендаций по устранению выявленных уязвимостей. Направление в адрес НКЦКИ (по запросу) результатов указанных мероприятий. При проведении сканирования информационных ресурсов доступных со стороны сети Интернет необходимо предварительное уведомление НКЦКИ (с использованием личного кабинета корпоративного центра, функционирующего в технической инфраструктуре НКЦКИ, электронной почты, а при отсутствии указанных каналов передачи информации – почтовых отправлений) не позднее, чем за 5 рабочих дней до предполагаемого дня проведения мероприятий, либо однократно, с указанием периодичности (графика) проведения таких мероприятий (в случае если мероприятия осуществляются систематически). В случае, если решение о проведении мероприятий принимается менее, чем за 5 рабочих дней до предполагаемого дня их проведения, допускается информировать НКЦКИ в день проведения мероприятий;

– проведение мероприятий по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак в отношении информационных ресурсов, находящихся в зоне ответственности *(наименование контрагента)*, а также направление в адрес НКЦКИ не позднее 5 календарных дней с момента завершения таких мероприятий их подробных результатов;

– передачу в НЦКЦИ сведений о консалтинговых услугах (наименование юридического лица или ФИО индивидуального предпринимателя, которому оказывались указанные услуги, ИНН, КПП, дата оказания услуги, предмет договора), не

позднее 5 календарных дней с момента заключения договора об оказании таких услуг;

– своевременное направление в адрес владельцев информационных ресурсов, находящихся в зоне ответственности *(наименование контрагента)*, информации, получаемой от НКЦКИ для информирования владельцев информационных ресурсов и о результатах, полученных в ходе исполнения положений настоящего Соглашения, а также соответствующих рекомендаций для устранения угроз информационной безопасности;

Предоставление в НКЦКИ сведений об информационных ресурсах, находящихся в зоне ответственности *(наименование контрагента)*, а также о результатах, полученных в ходе исполнения положений настоящего Соглашения, производится в соответствии с форматами обмена данными и в сроки, определенными в Регламенте взаимодействия Сторон при осуществлении информационного обмена.

2. НКЦКИ осуществляет:

– разработку совместно с корпоративным центром перечня информации, передаваемой в ходе взаимодействия Сторон в рамках настоящего Соглашения;

– разработку и передачу в *(наименование контрагента)* методических рекомендаций по обнаружению компьютерных атак, предупреждению и установлению причин компьютерных инцидентов, ликвидации последствий этих инцидентов, а также требований к документальным материалам, необходимым *(наименование контрагента)* в целях научно-технического обеспечения создания и функционирования корпоративного центра;

– согласование документальных материалов, разрабатываемых *(наименование контрагента)* в целях научно-технического обеспечения создания и функционирования корпоративного центра;

– участие в совместных мероприятиях по оценке степени защищенности от компьютерных атак информационных ресурсов, находящихся в зоне ответственности *(наименование контрагента)*;

– участие в мероприятиях по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак в отношении информационных ресурсов, находящихся в зоне ответственности *(наименование контрагента)*;

– доведение до *(наименование контрагента)* имеющихся сведений об угрозах информационной безопасности в отношении информационных ресурсов, находящихся зоне ответственности *(наименование контрагента)*, а также о мерах по нейтрализации данных угроз;

– взаимодействие с уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты;

– контроль за соблюдением корпоративным центром *(наименование контрагента)* требований к подразделениям и должностным лицам субъектов ГосСОПКА.

3. Период и порядок организации и проведения мероприятий, указанных в абзацах пятом и шестом пункта 2 настоящей статьи, определяются положениями Регламента взаимодействия Сторон при осуществлении контроля степени защищенности (данный Регламент заключается по решению НКЦКИ) и Регламента взаимодействия Сторон при осуществлении мероприятий по реагированию на компьютерные инциденты.

Регламенты, предусмотренные настоящей статьей, разрабатываются и утверждаются головными подразделениями, определенными в статье 3 настоящего Соглашения.

Статья 6

Деятельность Сторон, предусмотренная настоящим Соглашением, осуществляется безвозмездно.

Статья 7

Стороны обязуются сохранять конфиденциальную информацию и принимать все необходимые меры для ее защиты, в том числе в случае реорганизации или ликвидации

Сторон.

При этом под конфиденциальной информацией понимается информация, в отношении которой ее обладателем введен режим конфиденциальности и бумажный или электронный носитель такой информации содержит реквизиты, позволяющие однозначно ее отнести к конфиденциальной информации.

Стороны настоящим соглашаются, что не разгласят и не допустят разглашение конфиденциальной информации никаким третьим лицам без предварительного письменного согласия другой стороны.

Передача конфиденциальной информации третьим лицам в целях реализации функций НКЦКИ осуществляется при условии ее обязательного обезличивания. При этом под обезличиванием понимается отсутствие привязки к конкретным информационным ресурсам.

Статья 8

Настоящее Соглашение вступает в силу со дня подписания и действует бессрочно.

Настоящее Соглашение может быть расторгнуто по согласованию Сторон, а также по инициативе одной из Сторон с уведомлением об этом другой Стороны не позднее чем за три месяца до дня прекращения его действия.

Стороны при взаимном согласии могут вносить в настоящее Соглашение изменения, которые оформляются отдельными протоколами, являющимися его неотъемлемой частью.

В целях реализации положений настоящего Соглашения могут проводиться рабочие встречи, создаваться рабочие группы.

Все вопросы, возникающие при реализации настоящего Соглашения, решаются путем переговоров и консультаций между Сторонами.

Совершено в г. Москве ____ _____ 2025 г. в двух подлинных экземплярах, по одному экземпляру для каждой из Сторон. Оба экземпляра имеют одинаковую юридическую силу.

Директор НКЦКИ *(Должность руководителя)*

О.В. Скрябин *[И.О. Фамилия]*