Государственная регистрация
от 23.04.2024 ГР/339/2024

**МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ
И СВЯЗИ КАЛИНИНГРАДСКОЙ ОБЛАСТИ**

П Р И К А З

«23» апреля 2024 г. № 92

Калининград

**Об утверждении регламента
эксплуатации государственной информационной системы
Калининградской области «Центр управления безопасностью»**

В соответствии с постановлением Правительства Калининградской области от 25 декабря 2018 года № 799 «Об утверждении положения о Министерстве цифровых технологий и связи Калининградской области», п р и к а з ы в а ю:

1. Утвердить регламент эксплуатации государственной информационной системы Калининградской области «Центр управления безопасностью» согласно приложению к настоящему приказу.

2. Признать утратившим силу приказ Министерства цифровых технологий и связи Калининградской области от 15 июня 2021 года № 242 «Об утверждении Временного регламента взаимодействия между оператором и администратором информационной безопасности единой информационной телекоммуникационной сети Правительства Калининградской области, а также уполномоченным органом».

3. Настоящий приказ подлежит государственной регистрации и вступает в силу со дня его официального опубликования.

Заместитель Председателя Правительства
Калининградской области –
министр Л.Ш. Дараселия

Приложение
к приказу Министерства цифровых
технологий и связи
Калининградской области
от «23» апреля 2024 года № 92

РЕГЛАМЕНТ
эксплуатации государственной информационной системы Калининградской области «Центр управления безопасностью»

Глава 1. Общие положения

1. В настоящем регламенте используются следующие определения и сокращения:

ГИС «ЦУБ»	Государственная информационная система Калининградской области «Центр управления безопасностью»
ГКУ КО «ЦЦТ»	Государственное казенное учреждение Калининградской области «Центр цифровых технологий»
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ЕИТС	Единая информационно-телекоммуникационная сеть Правительства Калининградской области, созданная на основании постановления Правительства Калининградской области от 04.06.2018 № 301 «Об утверждении положения о единой информационно-телекоммуникационной сети Правительства Калининградской области»
ИБ	Информационная безопасность
Информационная инфраструктура	Совокупность серверного оборудования, системного и прикладного программного обеспечения, систем хранения данных, автоматизированных рабочих мест, периферийного оборудования, информационно-телекоммуникационной сети, являющаяся основой для функционирования информационных систем (в том числе информационных систем персональных данных, государственных информационных систем и информационных систем критической информационной инфраструктуры)
КА	Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на компоненты информационной инфраструктуры, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности, обрабатываемой такими компонентами
КИ	Компьютерный инцидент – факт нарушения и (или) прекращения функционирования компонента информационной инфраструктуры, и (или) нарушения безопасности, обрабатываемой таким объектом информации, в том числе произошедший в результате КА

Карточка КИ	Документ, содержащий формализованное описание КИ
Компонент информационной инфраструктуры	Программное, программно-аппаратное средство, выполняющее функции по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передаче (распространению, предоставлению доступа), блокированию, удалению, уничтожению данных в составе информационной инфраструктуры
МКИ	Менеджмент КИ, в ходе которого выполняются выявление, учет, регистрация, анализ, информирование, реагирование, устранение и закрытие инцидентов узлов безопасности, а также процессы инвентаризации
НКЦКИ	Национальный координационный центр по КИ – составная часть сил, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ
Ответственный за реагирование на КИ	Сотрудник пользователя ГИС «ЦУБ», ответственный за функционирование узла безопасности, а также за принятие мер по локализации КИ и устранение последствий КИ
Ответственный за принятие решений	Сотрудник пользователя ГИС «ЦУБ», уполномоченный на принятие решений по режиму функционирования узла безопасности, его архитектуре, а также по принятию мер, по локализации КИ, нарушающих нормальный режим функционирования узла безопасности
Приоритет КИ	Характеристика КИ, определяемая с учетом потенциального (возможного) негативного влияния КИ на узел безопасности, ЕИТС или инфраструктуру пользователя ГИС «ЦУБ» в целом, включая длительное полное прерывание работы, остановку функционирования отдельных процессов, нарушение конфиденциальности, целостности и(или) доступности обрабатываемых данных
Система анализа событий безопасности	Система, позволяющая на основе правил определить соответствие порядка и качества событий безопасности КИ ИБ
СКЗИ	Средства криптографической защиты информации, реализующие алгоритмы криптографического преобразования информации
Событие безопасности	Идентифицированное возникновение определенного состояния системы, сервиса или сети, указывающее (напрямую или косвенно) на возможное нарушение политики ИБ, отказ защитных мер или возникновение неизвестной ранее ситуации, которая может иметь отношение к ИБ.
Узел безопасности	Подключенный к ГИС «ЦУБ» компонент информационной инфраструктуры

2. Настоящий регламент определяет процессы эксплуатации ГИС «ЦУБ» и порядок взаимодействия участников в ходе выявления КИ, реагировании на КИ и принятии мер по ликвидации последствий КА.

3. К участникам в рамках настоящего регламента относятся:

1) уполномоченный орган – Министерство цифровых технологий и связи

Калининградской области, электронный адрес inform@gov39.ru;

2) оператор ГИС «ЦУБ» – ГКУ КО «ЦЦТ», электронный адрес helpdesk@gov39.ru;

3) оператор Единой информационно-телекоммуникационной сети Правительства Калининградской области – ГКУ КО «ЦЦТ», электронный адрес helpdesk@gov39.ru;

4) пользователи ГИС «ЦУБ» – органы исполнительной власти Калининградской области и подведомственные им государственные учреждения Калининградской области, а также органы местного самоуправления муниципальных образований Калининградской области и подведомственные им учреждения (организации), которые подключаются к ГИС «ЦУБ» на основании заключенных с уполномоченным органом и оператором ГИС «ЦУБ» соглашений.

4. ГИС «ЦУБ» применяется для реализации функций ведомственного центра ГосСОПКА.

5. Настоящий регламент разработан на основании положений, следующих нормативных правовых актов и документов:

1) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденная Президентом Российской Федерации 12.12.2014 № К 1274;

3) постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4) ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения»;

5) ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения»;

6) ГОСТ Р 59711-2022 «Защита информации. Организация деятельности по управлению компьютерными инцидентами»;

7) ГОСТ Р 59712-2022 «Защита информации. Руководство по реагированию на компьютерные инциденты»;

8) приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

9) приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

10) методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 24.12.2016 № 149/2/7-200

(документ ограниченного доступа);

11) требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденные НКЦКИ (документ ограниченного доступа);

12) Закон Калининградской области от 24.04.2018 № 165 «О правовом регулировании отдельных вопросов в сфере создания, модернизации и эксплуатации государственных информационных систем Калининградской области»;

13) постановление Правительства Калининградской области от 04.06.2018 № 301 «Об утверждении положения о единой информационно-телекоммуникационной сети Правительства Калининградской области»;

14) постановление Правительства Калининградской области от 10.11.2020 № 804 «О создании государственной информационной системы Калининградской области «Центр управления безопасностью»;

15) постановление Правительства Калининградской области от 05.08.2021 № 465 «О вводе в эксплуатацию государственной информационной системы Калининградской области «Центр управления безопасностью»;

16) приказ Министерства цифровых технологий и связи Калининградской области от 31.08.2021 № 366 «Об утверждении положения о государственной информационной системе Калининградской области «Центр управления безопасностью»;

17) приказ Министерства цифровых технологий и связи Калининградской области от 27.05.2020 № 216 «Об операторе единой информационно-телекоммуникационной сети Правительства Калининградской области».

Глава 2. Порядок подключения к ГИС «ЦУБ»

6. Для подключения к ГИС «ЦУБ» между участниками взаимодействия заключается Соглашение о подключении к ГИС «ЦУБ» по форме согласно приложению № 1 к настоящему регламенту (далее – Соглашение).

Пользователь ГИС «ЦУБ» направляет в адрес уполномоченного органа подписанное Соглашение в трех экземплярах. Уполномоченный орган и оператор ГИС «ЦУБ» в течение трех рабочих дней с даты получения Соглашения подписывают и направляют в адрес участника взаимодействия один экземпляр Соглашения или уведомляют пользователя ГИС «ЦУБ» об отказе в подписании Соглашения.

Пользователь ГИС «ЦУБ» в течение трех рабочих дней с даты получения подписанного уполномоченным органом и оператором ГИС «ЦУБ» Соглашения направляет оператору ГИС «ЦУБ» заявку на подключение к ГИС «ЦУБ» по форме согласно приложению № 2 к настоящему регламенту.

Информация, прикладываемая к заявке на подключение, подлежит передаче оператору ГИС «ЦУБ» на съемном носителе или по защищенным каналам связи в электронном виде (в форме электронного документа). Не допускается передача указанной информации по незащищенным каналам связи.

7. Подключение компонентов информационной инфраструктуры к процессу МКИ осуществляется согласно следующим этапам:

1) отнесение компонентов информационной инфраструктуры пользователя ГИС «ЦУБ» к узлам безопасности;

2) инвентаризация узлов безопасности и составление паспортов узлов безопасности;

3) разработка оператором ГИС «ЦУБ» требований по подключению узла безопасности к ГИС «ЦУБ»;

4) выполнение разработанных требований пользователем ГИС «ЦУБ», подключение узла безопасности к ГИС «ЦУБ» оператором ГИС «ЦУБ».

8. Отнесение компонента информационной инфраструктуры пользователя ГИС «ЦУБ» к узлу безопасности и его дальнейшее подключение к процессу МКИ осуществляется в порядке приоритета, обусловленного:

1) критичностью выполняемых компонентом информационной инфраструктуры / ЕИТС функций в приложении к свойствам безопасности обрабатываемой информации (конфиденциальность, целостность, доступность) в соответствии с требованиями, установленными нормативными правовыми актами Российской Федерации и Калининградской области по защите информации;

2) влиянием компонента информационной инфраструктуры / ЕИТС на другие компоненты информационной инфраструктуры / ЕИТС (на их возможность выполнять свои функции в штатном режиме);

3) возможным репутационным ущербом (в случае публичных сервисов).

9. Устанавливаются 3 уровня приоритета отнесения компонентов информационной инфраструктуры ЕИТС к узлам безопасности: «низкий», «средний» и «высокий».

Приоритет в отношении каждого рассматриваемого компонента определяется в соответствии со следующей таблицей (тот или иной уровень назначается в случае выполнения хотя бы одного из перечисленных критериев):

№ п/п	Высокий	Средний	Низкий
1	Отказ в обслуживании компонента информационной инфраструктуры может повлиять на работоспособность более 50 других компонентов информационной инфраструктуры / ЕИТС	Отказ в обслуживании компонента информационной инфраструктуры может повлиять на работоспособность не менее 10, но не более 50 других компонентов информационной инфраструктуры / ЕИТС	Отказ в обслуживании компонента информационной инфраструктуры может повлиять на работоспособность менее 10 других компонентов информационной инфраструктуры / ЕИТС
2	Компрометация компонента информационной инфраструктуры может привести к компрометации других компонентов информационной инфраструктуры, к утечке	Компрометация компонента информационной инфраструктуры может создать предпосылки к компрометации других компонентов информационной инфраструктуры, к утечке	Компрометация компонента информационной инфраструктуры не может создать предпосылки к компрометации других компонентов информационной

№ п/п	Высокий	Средний	Низкий
	конфиденциальной информации или остановке основных бизнес-процессов	конфиденциальной информации или остановке основных бизнес-процессов	инфраструктуры, но к свойствам информации, обрабатываемой на компоненте информационной инфраструктуры, предъявляются требования по обеспечению либо конфиденциальности, либо целостности, либо доступности
3	Компрометация компонента информационной инфраструктуры может нанести репутационный ущерб структурным подразделениям Правительства Калининградской области или органам исполнительной власти Калининградской области	Компрометация компонента информационной инфраструктуры может нанести репутационный ущерб подведомственному учреждению органа исполнительной власти Калининградской области	Компрометация компонента информационной инфраструктуры может нанести репутационный ущерб муниципальному образованию или подведомственному учреждению муниципального образования Калининградской области

10. Пользователь ГИС «ЦУБ» и оператор ГИС «ЦУБ» определяют функциональные категории компонентов информационной инфраструктуры, которым присваивается приоритет отнесения к узлам безопасности.

11. По согласованию с пользователем ГИС «ЦУБ» может быть разработан план подключения узлов безопасности к ГИС «ЦУБ».

12. Пользователь ГИС «ЦУБ» согласно приоритетам функциональных категорий информационной инфраструктуры и/или плану подключения в ГИС «ЦУБ» проводит инвентаризацию и заполняет информацию о компоненте информационной инфраструктуры в паспорте узла безопасности по форме согласно приложению № 3 к настоящему регламенту.

При необходимости, пользователь ГИС «ЦУБ» запрашивает необходимую информацию у оператора ЕИТС и/или оператора ГИС «ЦУБ».

Паспорт узла безопасности направляется оператору ГИС «ЦУБ» с фиксацией данных о его получении. Оператор ГИС «ЦУБ» идентифицирует компонент информационной инфраструктуры как узел безопасности.

13. С момента получения паспорта узла безопасности оператор ГИС «ЦУБ», в срок не более чем два рабочих дня, рассматривает и принимает паспорт узла безопасности и формирует требования по подключению к ГИС «ЦУБ», направляет их в адрес пользователя ГИС «ЦУБ».

14. Пользователь ГИС «ЦУБ» с момента получения требований по подключению в течение двух рабочих дней выполняет требования оператора ГИС «ЦУБ» и отправляет ему ответ, содержащий информацию о выполнении требований, а при необходимости, дополнительные сведения об узле безопасности.

15. В случае невозможности подключения узла безопасности в ГИС «ЦУБ» оператор ГИС «ЦУБ» в течение двух рабочих дней с момента получения паспорта узла безопасности уведомляет пользователя ГИС «ЦУБ», уполномоченный орган с указанием объективных причин отказа в подключении.

16. В случае выявления оператором ГИС «ЦУБ» компонента информационной инфраструктуры, параметры которого подпадают под критерии отнесения к узлам безопасности, но не отнесенного к узлу безопасности, оператор ГИС «ЦУБ» сообщает об этом соответствующему пользователю ГИС «ЦУБ». Пользователь ГИС «ЦУБ» в течении двух рабочих дней локализует неучтённый компонент информационной инфраструктуры и направляет в адрес оператора ГИС «ЦУБ» информацию о неучтённом узле и предполагаемом уровне приоритета для его согласования и последующего описания, а также определения сроков его паспортизации.

17. С целью систематизации информации о ресурсах, включаемых в процесс МКИ, пользователь ГИС «ЦУБ» разрабатывает структурную схему собственной информационной инфраструктуры, отражая все существующие и вновь включаемые в процесс МКИ узлы безопасности. Указанные схемы поддерживаются в актуальном состоянии пользователем ГИС «ЦУБ» и передаются оператору ГИС «ЦУБ» при внесении изменений в указанную схему в срок, не превышающий двух рабочих дней с момента этих изменений или по запросу оператора.

18. В случае необходимости внесения изменений в параметры функционирования узла безопасности или же иного оборудования, влияющего на процесс его функционирования, пользователь ГИС «ЦУБ» заблаговременно (не менее одного рабочего дня) уведомляет оператора ГИС «ЦУБ» о планируемых изменениях параметров, а также о результатах внесения указанных изменений. При этом пользователь ГИС «ЦУБ» в течение двух рабочих дней заполняет и направляет в адрес оператора ГИС «ЦУБ» обновленный паспорт узла безопасности в части произведенных изменений. Пользователь ГИС «ЦУБ» при внесении любых изменений обеспечивает доступность оператору ГИС «ЦУБ» узлов безопасности.

Глава 3. Порядок отключения от ГИС «ЦУБ»

19. В случае, если пользователь ГИС «ЦУБ» не считает необходимым МКИ в отношении отдельных подключенных узлов безопасности в связи с утратой актуальности, выведения из эксплуатации узла безопасности и в иных случаях, пользователь ГИС «ЦУБ» направляет оператору ГИС «ЦУБ» заявку об отключении узлов безопасности от ГИС «ЦУБ» с указанием причины.

20. При получении заявки, описанной в пункте 19 настоящего регламента, оператор ГИС «ЦУБ» производит необходимые операции по исключению узлов безопасности из процесса МКИ в срок, не превышающий один рабочий день.

21. В случае, если оператор ГИС «ЦУБ» не считает необходимым МКИ в отношении отдельных подключенных узлов безопасности в связи с перераспределением вычислительных или технологических мощностей оператора ГИС «ЦУБ» для включения в процесс МКИ более критичных узлов

безопасности, он уведомляет пользователя ГИС «ЦУБ» об отключении узлов безопасности от ГИС «ЦУБ».

22. В случае, если оператором ГИС «ЦУБ» выявлено нарушение положений настоящего регламента пользователем ГИС «ЦУБ» или в случае выявления фактов деструктивных действий по отношению к ГИС «ЦУБ», оператор ГИС «ЦУБ» направляет пользователю ГИС «ЦУБ» и уполномоченному органу уведомление о выявленных нарушениях. В зависимости от обстоятельств нарушения, оператором ГИС «ЦУБ» принимается решение об исключении узлов безопасности.

Глава 4. Основные положения по МКИ

23. Основной целью МКИ является повышение уровня защищенности информационных систем, вычислительных ресурсов и информационно-телекоммуникационной инфраструктуры пользователей ГИС «ЦУБ», а также компонентов ЕИТС.

24. Основными задачами МКИ являются:

1) взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий КА на информационные ресурсы и реагирования на КИ, в том числе в части информационно-аналитического и прогностического обеспечения функционирования ГосСОПКА, предоставление в НКЦКИ сведений о состоянии защищенности информационных ресурсов от КА и информации о КИ в соответствии с установленным порядком;

2) разработка документов, регламентирующих процессы обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ;

3) эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, выявление ошибок в работе средств защиты информации и направление производителю данных средств информации о выявленных ошибках, а также актуализация средств защиты информации, используемых для обеспечения защиты информационных ресурсов, направление в НКЦКИ предложений по совершенствованию средств защиты информации;

4) прием сообщений о КИ от пользователей информационных ресурсов;

5) регистрация КА и КИ;

6) анализ событий ИБ;

7) инвентаризация информационных ресурсов;

8) анализ угроз ИБ, прогнозирование их развития и направление в НКЦКИ результатов;

9) составление и актуализация перечня угроз ИБ для информационных ресурсов;

10) выявление уязвимостей информационных ресурсов;

11) формирование предложений по повышению уровня защищенности информационных ресурсов;

12) составление перечня КИ;

13) ликвидация последствий КИ;

14) анализ результатов ликвидации последствий КИ;

15) установление причин КИ.

Схема процессов МКИ представлена на рисунке 1.

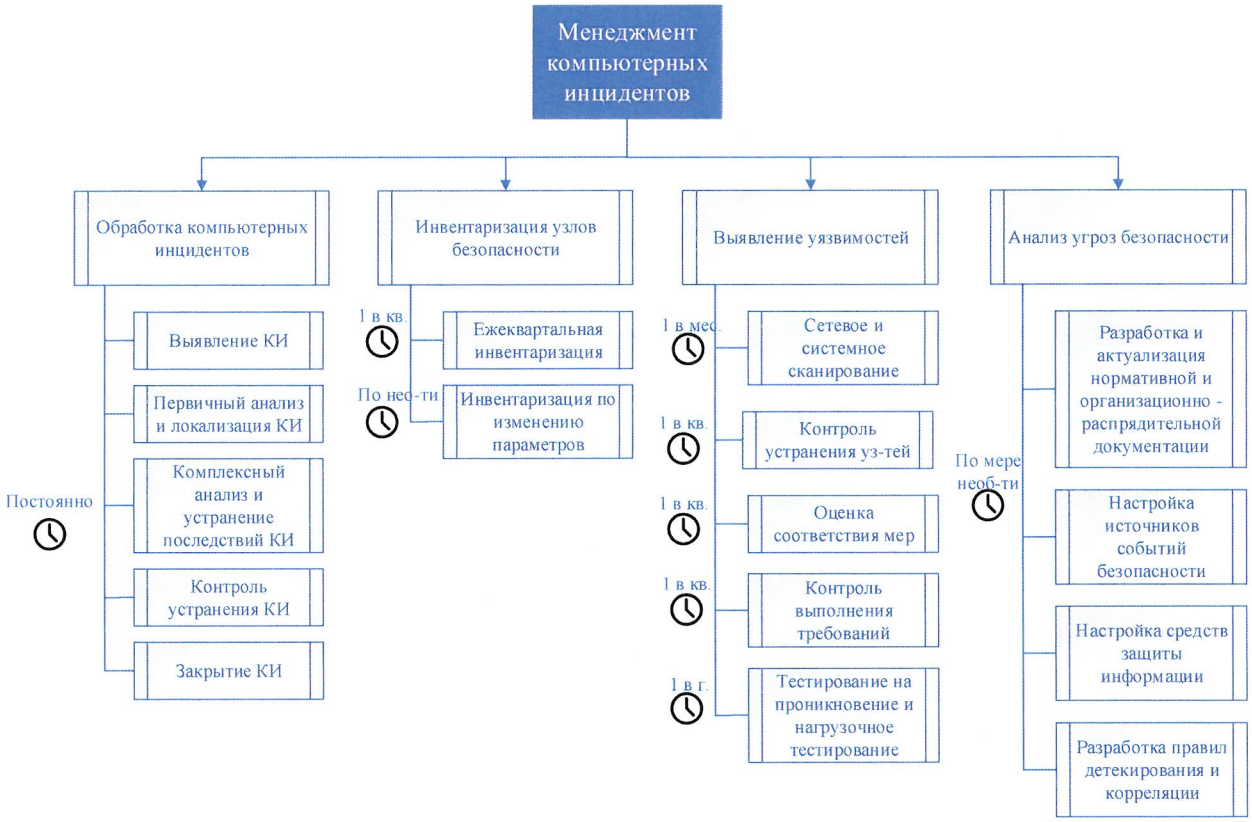

Рисунок 1 – Схема процессов МКИ

25. Оператор ГИС «ЦУБ» осуществляет МКИ на основе информации, получаемой с узлов безопасности информационной инфраструктуры пользователя ГИС «ЦУБ» и ЕИТС или по сообщениям, получаемым от НКЦКИ и/или пользователя ГИС «ЦУБ».

26. К узлам безопасности относятся следующие компоненты информационной инфраструктуры пользователя ГИС «ЦУБ» и ЕИТС, информация о которых содержится в паспортах узлов безопасности по форме согласно приложению № 3 к настоящему регламенту:

1) серверное оборудование и системы хранения данных;
2) активное сетевое оборудование;
3) автоматизированные рабочие места пользователей;
4) активное периферийное оборудование;
5) общесистемное и специализированное программное обеспечение;
6) средства защиты информации;
7) средства антивирусной защиты;
8) средства управления информацией об угрозах безопасности информации;
9) системы контроля защищенности и соответствия стандартам;
10) средства обнаружения вторжений;
11) средства защиты информации среды виртуализации;
12) средства межсетевого экранирования;
13) системы защиты приложений от несанкционированного доступа;
14) системы анализа сетевого трафика.

27. Пользователем ГИС «ЦУБ» осуществляется контроль и учет компонентов информационной инфраструктуры пользователя ГИС «ЦУБ», при этом на каждый компонент, отнесенный к узлу безопасности, формируется паспорт узла безопасности по форме согласно приложению № 3 к настоящему регламенту.

28. Функции пользователя ГИС «ЦУБ»:

1) утверждает и поддерживает в актуальном состоянии организационно-распорядительные документы на систему защиты информации;

2) совместно с оператором ГИС «ЦУБ» определяет состав компонентов информационной инфраструктуры, подключаемых в процесс МКИ;

3) совместно с оператором ГИС «ЦУБ» организует инвентаризацию узлов безопасности и их паспортизацию;

4) организует приоритезацию (включения) подключения узлов безопасности в процесс МКИ;

5) обеспечивает работоспособность и конфигурирование узлов безопасности, а также вспомогательного аппаратного, программного и телекоммуникационного обеспечения, необходимого для подключения к ГИС «ЦУБ»;

6) по запросам оператора ГИС «ЦУБ» предоставляет необходимую информацию для подтверждения и устранения КИ;

7) по рекомендации оператора ГИС «ЦУБ» обеспечивает устранение КИ и их последствий;

8) обеспечивает актуальность информации об узлах безопасности, переданной в ГИС «ЦУБ», проводит периодическую их инвентаризацию;

9) выявляет потенциальные КА и КИ из источников событий безопасности, недоступных для оператора ГИС «ЦУБ»;

10) в рамках своей компетенции устраняет выявленные оператором ГИС «ЦУБ» уязвимости узлов безопасности.

29. Функции оператора ГИС «ЦУБ»:

1) взаимодействует с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий КА на информационные ресурсы и реагирования на КИ, в том числе в части информационно-аналитического и прогностического обеспечения функционирования ГосСОПКА, предоставляет в НКЦКИ сведения о состоянии защищенности информационных ресурсов от КА и информацию о КИ. При этом руководствуется следующими документами:

- Порядком обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты и Порядком получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения, утвержденными приказом ФСБ России от 24.07.2018 № 368;

- Перечнем информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядком представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденными приказом ФСБ России от 24.07.2018 № 367;

- Порядком информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСБ России от 19.06.2019 № 282;

2) консультирует пользователя ГИС «ЦУБ» в процессе осуществления МКИ;

3) участвует в процессе инвентаризации узлов безопасности и организует их подключение к ГИС «ЦУБ»;

4) обеспечивает функционирование оборудования и программного обеспечения ГИС «ЦУБ»;

5) на основе получаемых от узлов безопасности пользователя ГИС «ЦУБ» и оператора ЕИТС событий безопасности проводит их анализ и выявляет КА и потенциальные КИ;

6) принимает сообщения о КИ или КА от пользователей ГИС «ЦУБ»;

7) во взаимодействии с пользователем ГИС «ЦУБ» подтверждает КИ;

8) регистрирует КА и КИ;

9) вырабатывает рекомендации по локализации и устранению КИ на узлах безопасности информационной инфраструктуры пользователя ГИС «ЦУБ»;

10) контролирует процесс устранения КИ;

11) в рамках своей компетенции учувствует в процессе устранения КИ;

12) составляет перечень КИ;

13) устанавливает причины КИ;

14) осуществляет анализ уязвимостей узлов безопасности информационной инфраструктуры пользователей ГИС «ЦУБ»;

15) вырабатывает рекомендации по устранению выявленных уязвимостей информационной инфраструктуры пользователей ГИС «ЦУБ»;

16) производит контроль устранения уязвимостей информационной инфраструктуры пользователей ГИС «ЦУБ»;

17) производит анализ угроз ИБ, прогнозирует их развитие;

18) разрабатывает методические рекомендации по реализации комплекса мероприятий по обнаружению, предупреждению и ликвидации последствий типовых КИ, формирует предложения по повышению уровня защищенности узлов безопасности.

30. Функции уполномоченного органа:

1) согласовывает и координирует подключение пользователей к ГИС «ЦУБ»;

2) утверждает и поддерживает в актуальном состоянии организационно-распорядительные документы на систему защиты информации ЕИТС, а также нормативные правовые акты, регулирующие функционирование ГИС «ЦУБ»;

3) принимает участие в устранении КИ в части согласования обновления,

остановки, изоляции или реорганизации вовлеченных в КА или КИ узлов безопасности или же узлов потенциально подверженные КА.

31. Функции оператора ЕИТС:

1) в пределах компетенции осуществляет работы по организации сетевой связности узлов безопасности пользователей ГИС «ЦУБ» и ГИС «ЦУБ»;

2) в пределах компетенции является пользователем ГИС «ЦУБ» и выполняет функции пользователя ГИС «ЦУБ» в рамках администрируемых компонентов ЕИТС.

32. Обмен информацией между оператором ГИС «ЦУБ», пользователем ГИС «ЦУБ» и уполномоченным органом может осуществляться:

1) по электронной почте;

2) по телефонной связи;

3) с использованием систем по обработке заявок пользователей;

4) с использованием специализированных информационных систем по МКИ и автоматизации процессов реагирования.

33. Участникам запрещается передавать информацию конфиденциального характера по открытым каналам связи без использования СКЗИ каналов связи.

Глава 5. Порядок обработки КИ

34. Обработка КИ в процессе МКИ посредством ГИС «ЦУБ» состоит из следующих этапов:

1) выявление КИ: анализ событий безопасности (в т.ч. о КА), поступающих от источников выявления КИ или от пользователя ГИС «ЦУБ», определение КИ в системе анализа событий безопасности (SIEM) по заданным правилам корреляции, его регистрация и классификация, создание карточки КИ;

2) первичный анализ и локализация КИ: подтверждение КИ, оценка критичности (приоритезация устранения КИ), выявление источника возникновения и участников КИ, при необходимости запрос необходимых сведений, определение исполнителя, информирование ответственного за реагирование на КИ, передача информации о КИ в НКЦКИ;

3) комплексный анализ и устранение последствий: выявление причин возникновения КИ, определение потенциальных подверженных КИ ресурсов, фиксация следов нарушителя, формирование алгоритма устранения КИ и его последствий, исполнение указанного алгоритма, в том числе устранение причин возникновения КИ, уведомление НКЦКИ о принятых мерах;

4) контроль устранения: анализ событий безопасности, поступающих от источника, зафиксировавшего КИ и другим косвенным признакам, на предмет соответствия параметрам КИ, при необходимости уведомление НКЦКИ;

5) закрытие КИ: перевод статуса КИ в статус «закрытый», фиксация сведений о принятых мерах для устранения КИ, при необходимости формирование методических рекомендаций (бюллетеня информационной безопасности), уведомление НКЦКИ (в случае необходимости), уведомление пользователей ГИС «ЦУБ», чьи ресурсы могут быть подвержены аналогичным КИ.

На рисунке 2 изображена обобщенная схема взаимодействия оператора, где:

ОГ) – Оператор ГИС «ЦУБ»,
ОЕ) – Оператор ЕИТС;
П) – Пользователь ГИС «ЦУБ»;
ВУ – время устранения;
ВР – время реакции.

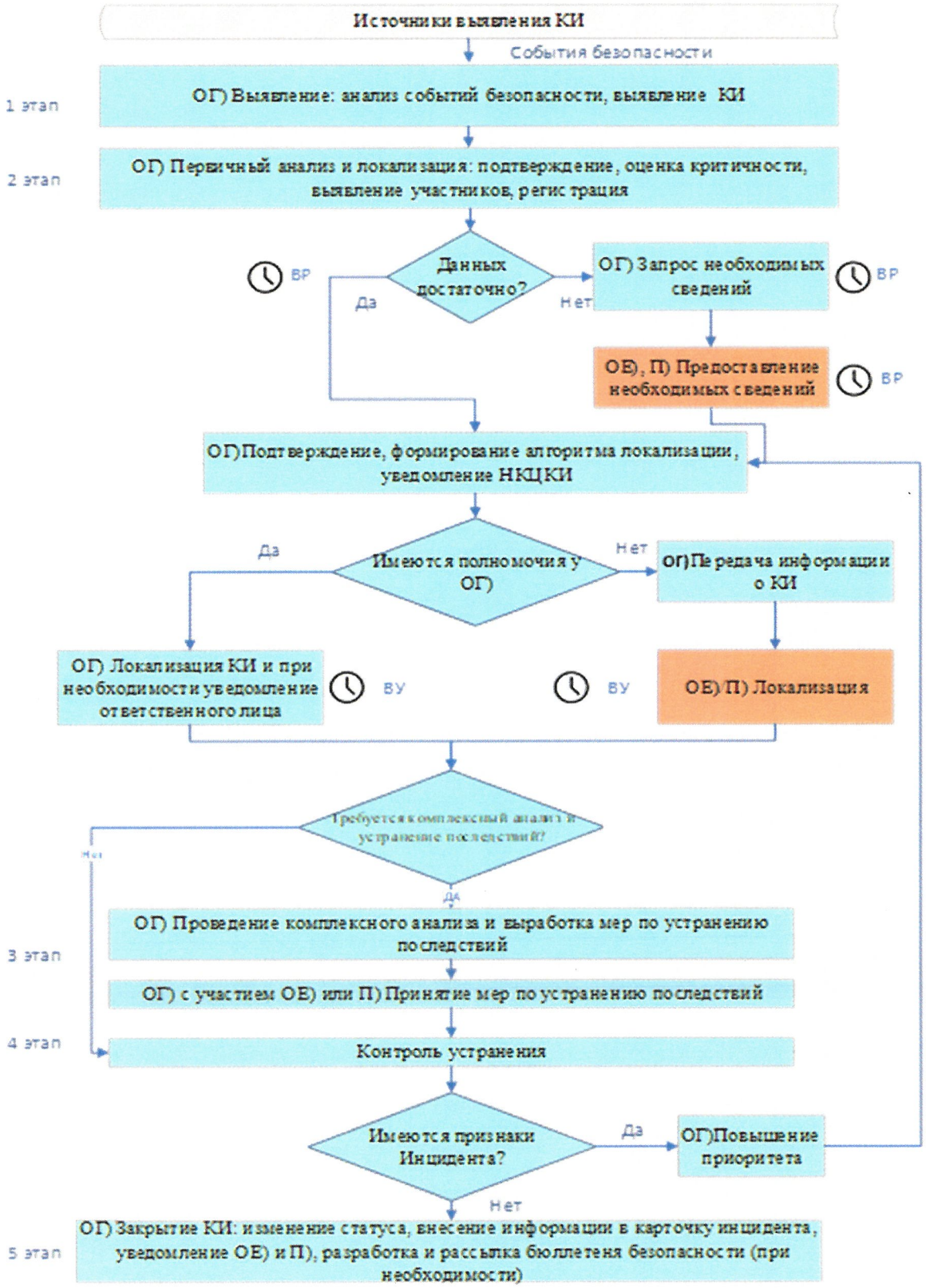

Рисунок 2 – Обобщенная схема взаимодействия оператора ГИС «ЦУБ» и оператора ЕИТС/пользователя ГИС «ЦУБ» по обработке КИ ИБ.

35. Порядок выявления КИ.

Выявление КИ производится оператором ГИС «ЦУБ» исходя из информации, полученной из следующих источников событий безопасности:

1) события из журналов безопасности, поступающие в систему анализа событий безопасности (SIEM) от узлов безопасности;

2) информация о КА, поступающая: из систем обнаружения и предотвращения вторжений, антивирусных средств защиты информации, средств защиты от несанкционированного доступа, средства защиты среды виртуализации, установленных в ЕИТС или инфраструктуре пользователя ГИС «ЦУБ»;

3) средства анализа уязвимостей;

4) система обнаружения вторжений ГосСОПКА;

5) иные, включая деятельность оператора ЕИТС, пользователя ГИС «ЦУБ» и пользователей информационной инфраструктуры пользователя ГИС «ЦУБ», посредством передачи сообщений.

36. В случае обнаружения КИ на компоненте информационной инфраструктуры пользователя ГИС «ЦУБ», не являющемся узлом безопасности, приоритет по устранению данного КИ устанавливается не выше «средний».

37. В случае необходимости присвоения КИ приоритета «высокий» или «очень высокий» в отношении компонента информационной инфраструктуры пользователя ГИС «ЦУБ», не отнесенного к узлу безопасности, оператор ГИС «ЦУБ» направляет запрос пользователю ГИС «ЦУБ» на заполнение и передачу паспорта узла безопасности на данный компонент. Ответ на указанный запрос пользователь ГИС «ЦУБ» предоставляет в срок, не превышающий времени реакции на КИ.

38. В случае обнаружения признаков КИ пользователем ГИС «ЦУБ», указанные признаки передаются оператору ГИС «ЦУБ» с целью проведения исследования на предмет соответствия КИ ИБ. Пользователь ГИС «ЦУБ» передает следующую информацию о КИ:

1) контактную информацию лица, сообщившего о КИ (если автор сообщения согласен предоставить такую информацию);

2) наименование информационных ресурсов, вовлеченных в КИ, а при невозможности такой идентификации – любые сведения, позволяющие прямо или косвенно определить такие ресурсы;

3) время обнаружения КИ;

4) характер КИ, как его понимает и может сформулировать автор сообщения;

5) сведения о принятых мерах, которыми располагает автор сообщения.

39. При получении сообщения оператор ГИС «ЦУБ» проводит регистрацию КИ путем создания карточки КИ, в которую вносит все полученные сведения независимо от их полноты и достоверности.

40. Выявление КИ производится оператором ГИС «ЦУБ» на основании данных источников событий безопасности и системы анализа событий безопасности, с учётом данных о типе узла безопасности, используемого прикладного и общесистемного программного обеспечения, а также типовых правил обнаружения КИ (правил корреляции).

41. Для применения нестандартных правил выявления КИ

(правил корреляции) в отношении определенного узла пользователь ГИС «ЦУБ» совместно с оператором ГИС «ЦУБ» формирует специфический для определённого узла (группы узлов ИБ) набор требований к очередности и качеству событий безопасности, поступающих от источников событий безопасности, которые необходимо считать КИ для данного узла безопасности, с указанием причин отнесения данной информации к КИ.

42. По факту получения требований для формирования нестандартных правил выявления КИ (правил корреляции) оператор ГИС «ЦУБ» организует их технологическую реализацию на подходящем источнике событий безопасности или же на техническом средстве, реализующем анализ событий с необходимого источника, в срок не превышающий 14 рабочих дней самостоятельно или же с привлечением специалистов производителя указанного источника или технического средства, производящего анализ событий с необходимого источника. По факту реализации указанных правил оператор ГИС «ЦУБ» уведомляет пользователя ГИС «ЦУБ».

43. В случае невозможности или затруднения реализации указанных нестандартных правил выявления КИ, оператор ГИС «ЦУБ» в срок, не превышающий семи рабочих дней, уведомляет об этом пользователя ГИС «ЦУБ», а также уполномоченный орган с указанием объективных причин.

44. По факту выявления КИ на узле безопасности оператор ГИС «ЦУБ» приступает к первичному анализу и локализации КИ. В случае если КИ автоматизировано не сформирован в системе анализа событий информации (SIEM) оператор ГИС «ЦУБ» создает карточку КИ в данной системе и при необходимости вносит в нее параметры событий безопасности, которые первично относят их к КИ.

45. Первичный анализ и локализация КИ.

Для подтверждения КИ оператор ГИС «ЦУБ» анализирует события безопасности, которые относятся к данному КИ, и сопоставляет их с деятельностью и характеристиками узла безопасности, отраженными в паспорте узла безопасности, а также в иных доступных источниках. По результатам данного анализа оператор ГИС «ЦУБ» принимает решение о подтверждении КИ.

46. Для подтвержденного КИ оператор ГИС «ЦУБ» устанавливает приоритет КИ исходя из приоритета компонента информационной инфраструктуры, установленный при отнесении его к узлу безопасности, и экспертной оценки.

Критерий КИ	**Приоритет КИ**				
	Незначимый	*Низкий*	*Средний*	*Высокий*	*Очень высокий*
Видимый ущерб активу	Нет	Нет	Нет	Нет	Высокий
Потенциальный ущерб активу	Низкий	Низкий	Средний	Высокий	Высокий
Влияние на информационные процессы в момент КИ	Нет	Нет	Нет	Да	Да
Возможность спрогнозировать величины ущерба	Да	Да	Да	Да	Нет

Критерии реакции	**Уровень КИ**				
	Незначимый	*Низкий*	*Средний*	*Высокий*	*Критический*
Время реакции	По мере возможности	4 ч.	2 ч.	30 мин.	Немедленно
Время устранения КИ	По мере возможности	48 ч.	12 ч.	4 ч.	до 1 ч.

Примечание: время устранения КИ может превышать указанное, если работы по устранению КИ на узле безопасности не возможны без прерывания критичного функционального процесса или по иным объективным причинам.

47. Для выявления причин и первоначального источника появления КИ оператор ГИС «ЦУБ» анализирует события безопасности в хронологическом порядке и сопоставляет их с иными событиями безопасности подобного типа. В случае если КИ ИБ может быть следствием эксплуатации конкретного типа уязвимости, оператор ГИС «ЦУБ» делает анализ уязвимостей узла на предмет поиска данного конкретного типа уязвимостей.

48. Для выявления массовости КИ (несколько подтвержденных КИ на группу узлов безопасности), а также возможной эскалации КИ на иные узлы безопасности или компоненты информационной инфраструктуры пользователя ГИС «ЦУБ», оператор ГИС «ЦУБ» проводит выявление участвующих в КИ узлов безопасности. В ходе данных мероприятий оператор ГИС «ЦУБ» анализирует события безопасности на иных узлах безопасности на предмет совпадения по признакам выявленного КИ. Также в случае, если выявленный КИ имеет отношение с возможным получением прав доступа на узле безопасности, оператор ГИС «ЦУБ» проводит работы по выявлению подозрительной активности на этом узле безопасности и анализирует состояние узла безопасности на предмет признаков компрометации.

49. В случае если каких-либо сведений недостаточно для выполнения работ согласно пунктам 45 – 48 настоящего регламента, оператор ГИС «ЦУБ» формирует запрос на предоставление информации пользователю ГИС «ЦУБ» или оператору ЕИТС (в зоне его ответственности) с указанием конкретных видов информации и предварительным приоритетом КИ. Оператор ЕИТС / пользователь ГИС «ЦУБ» предоставляет оператору ГИС «ЦУБ» указанную информацию в срок, не превышающий время реакции на КИ в соответствии с установленным приоритетом КИ.

50. В случае не подтверждения КИ, по которому проводился анализ, оператором ГИС «ЦУБ» он переводится в статус «закрытый». В карточку КИ вносится информация, являющаяся ключевой в ходе не подтверждения КИ. Оператор ГИС «ЦУБ» корректирует правила выявления КИ (сигнатуры или правила корреляции SIEM) с целью недопущения подобных ложных срабатываний.

51. По результатам выполнения пунктов 45 – 48 настоящего регламента и при необходимости выполнения пункта 49 оператор ГИС «ЦУБ» формирует алгоритм локализации КИ, содержащий в себе набор и последовательность

первоочередных действий, направленных на прекращение деструктивного влияния КИ на узел безопасности, информационную инфраструктуру пользователя ГИС «ЦУБ» и/или ЕИТС.

52. Оператор ГИС «ЦУБ» в пределах имеющихся полномочий определяет может ли устранить КИ самостоятельно или же для устранения потребуется привлечение пользователя ГИС «ЦУБ» или оператора ЕИТС.

53. В случае если оператор ГИС «ЦУБ» обладает полномочиями по реализации мер по локализации выявленного КИ, оператором принимает меры по локализации КИ самостоятельно в срок, не превышающий время устранения КИ. В случае, если алгоритм локализации может повлиять на работоспособность/доступность узла безопасности и/или других компонентов информационной инфраструктуры пользователя ГИС «ЦУБ» или ЕИТС, оператор ГИС «ЦУБ» в оперативном порядке уведомляет ответственных за функционирование узла безопасности лиц (ответственного за принятие решений и ответственного за реагирование на КИ).

54. В случае, если оператору ГИС «ЦУБ» требуется привлечение к локализации КИ оператора ЕИТС или пользователя ГИС «ЦУБ», то оператор ГИС «ЦУБ» направляет ответственному за реагирование на КИ информацию о регистрационном номере КИ, узле безопасности, на котором произошел КИ, времени фиксирования, характере и описании КИ, а также инструкцию по локализации КИ в срок не превышающий время реакции на КИ согласно приоритету КИ. В случае если алгоритм локализации может повлиять на работоспособность/доступность узла безопасности и/или других компонентов информационной инфраструктуры пользователя ГИС «ЦУБ» или ЕИТС, оператор ГИС «ЦУБ» уведомляет ответственное лицо по принятию решений о необходимости принятия мер по локализации КИ.

55. Оператор ЕИТС или пользователь ГИС «ЦУБ» с момента получения информации по КИ уведомляет оператора ГИС «ЦУБ» о принятии заявки, назначенном сотруднике (в случае переназначения ответственным за реагирование на КИ) для устранения КИ и его контактных данных (электронная почта, номер мобильного телефона) в срок, не превышающий время реакции на КИ в соответствии с приоритетом КИ. Также оператор ЕИТС или пользователь ГИС «ЦУБ» принимает меры по локализации КИ и уведомляет оператора ГИС «ЦУБ» в срок, не превышающий время устранения КИ в соответствии с установленным приоритетом КИ.

56. Информация по пунктам 45 – 55 настоящего регламента вносится в карточку КИ с целью дальнейшего учета. Также оператор ГИС «ЦУБ» информирует НКЦКИ о КИ в срок, не превышающий 24 часа с момента обнаружения КИ.

57. В случае выявления критических, с точки зрения оператора ГИС «ЦУБ», уязвимостей или параметров, влияющих на безопасность, для устранения указанных уязвимостей и изменения параметров, оператором ГИС «ЦУБ» устанавливается КИ приоритет не ниже «высокий».

58. Комплексный анализ и устранение последствий.

Комплексный анализ и устранение последствий проводятся

преимущественно для КИ уровней критичности «высокий» и «очень высокий», а также иных КИ, в ходе локализации которых потребовалось применить меры локализации, влияющие на работоспособность/доступность узла безопасности и/или других компонентов информационной инфраструктуры пользователя ГИС «ЦУБ» или ЕИТС. Также комплексный анализ и устранение последствий проводятся для КИ, для устранения которых мер локализации по объективным причинам недостаточно.

59. В ходе комплексного анализа оператором ГИС «ЦУБ» во взаимодействии с оператором ЕИТС или пользователем ГИС «ЦУБ» устанавливаются причины КИ, фактические последствия. Детектируются следы действия нарушителя, анализируются возможные пути развития КИ, фиксируются связанные события безопасности (в том числе потенциально связанные КА), запрашиваются объяснения и собираются объективные подтверждения (снимки экранов, тексты электронных сообщений, фрагменты записей сетевого трафика).

60. Для проведения комплексного анализа оператор ГИС «ЦУБ» вправе запросить у пользователя ГИС «ЦУБ» и/или оператора ЕИТС непосредственные доступы на узел безопасности и связанные с КИ компоненты информационной инфраструктуры или ЕИТС для сбора сведений. Также оператор ГИС «ЦУБ» вправе запросить копии носителей информации узлов безопасности и компонентов информационной инфраструктуры или по возможности образов узлов безопасности, а также иную необходимую информацию.

61. Пользователь ГИС «ЦУБ» и/или оператор ЕИТС предоставляет необходимую информацию и доступы оператору ГИС «ЦУБ» в срок, не превышающий время реакции на КИ в соответствии с приоритетом КИ, или информирует об иных сроках их предоставления, при наличии объективных причин увеличения сроков с указанием таких причин.

62. По факту получения необходимых доступов и информации оператор ГИС «ЦУБ» проводит комплексный анализ и формирует алгоритм устранения последствий, точки контроля и мероприятия, направленные на устранение последствий КИ, в том числе на:

1) устранение возможности развития и эскалации КИ;

2) прекращение установленного или потенциального несанкционированного доступа;

3) устранение причин возникновения КИ;

4) восстановление работоспособности/доступности узла безопасности и связанных с ним компонентов информационной инфраструктуры и/или ЕИТС.

63. Оператор ГИС «ЦУБ» передает алгоритм устранения последствий КИ пользователю ГИС «ЦУБ» и/или оператору ЕИТС. Пользователь ГИС «ЦУБ» и/или оператор ЕИТС во взаимодействии с оператором ГИС «ЦУБ» выполняет меры по устранению последствий КИ, передавая информацию по выполнению его пунктов оператору ГИС «ЦУБ» согласно определенным в алгоритме точкам контроля.

64. Контроль устранения КИ ИБ.

По факту получения информации о выполнении всех операций,

перечисленных в алгоритме устранения последствий КИ или локализации КИ, для которого не требуется комплексный анализ и устранение последствий, оператор ГИС «ЦУБ» производит контроль устранения КИ, заключающийся в анализе событий безопасности, поступающих от источника, зафиксировавшего КИ и других косвенных признаков, на предмет соответствия параметрам КИ в срок, не превышающий срок устранения КИ в соответствии с его приоритетом.

65. В случае обнаружения признаков КИ оператор ГИС «ЦУБ» осуществляет дополнительный анализ КИ с определением расширенного алгоритма устранения КИ с уведомлением ответственного за принятие решений и ответственного за реагирование на КИ в срок, не превышающий время устранения КИ в соответствии с его приоритетом. Мероприятия по локализации КИ принимаются оператором ГИС «ЦУБ», пользователем ГИС «ЦУБ» или оператором ЕИТС в зависимости от имеющихся у указанных лиц полномочий немедленно. Оператор ГИС «ЦУБ» вносит соответствующую информацию в карточку КИ. Оператор ГИС «ЦУБ» информирует НКЦКИ о продолжении вредоносной активности в КИ.

66. Приоритет устранения КИ, который не удалось устранить операциями локализации КИ и мерами по устранению последствий КИ, устанавливается на уровень выше изначального (кроме приоритета «очень высокий»).

67. В случае необнаружения признаков КИ в соответствии с пунктом 64 настоящего регламента оператор ГИС «ЦУБ» уведомляет ответственного за принятие решений и ответственного за реагирование на КИ о подтверждении устранения КИ, при условии их участия в процессе обработки КИ.

68. Порядок закрытия КИ ИБ.

По факту подтверждения закрытия КИ оператор ГИС «ЦУБ» в карточке КИ переводит его статус в статус «Закрытый», а также вносит информацию о принятых мерах с приложением материалов их подтверждающих. Оператор ГИС «ЦУБ» уведомляет НКЦКИ о закрытии КИ.

69. В случае наличия предпосылок для возникновения подобных закрытому КИ иных КИ на других узлах безопасности оператор ГИС «ЦУБ» формирует бюллетень информационной безопасности, описывающий предпосылки для возникновения КИ и меры по его предупреждению. Оператор ГИС «ЦУБ» направляет данный бюллетень в адреса пользователей ГИС «ЦУБ», оператора ГИС «ЦУБ» и уполномоченного органа.

70. В случае необходимости оператор ГИС «ЦУБ» вносит корректировки настроек источников событий безопасности и(или) систем анализа событий безопасности с целью оперативного обнаружения КИ подобных закрытому.

Глава 6. Порядок инвентаризации узлов безопасности

71. Целью инвентаризации узлов безопасности является получение оператором ГИС «ЦУБ» и поддержание в актуальном состоянии сведений об узлах безопасности, подключенных к ГИС «ЦУБ», необходимых

для выполнения функций ведомственного центра ГосСОПКА, а также обеспечения непрерывного процесса МКИ.

72. Инвентаризация проводится пользователем ГИС «ЦУБ» при необходимости с привлечением оператора ГИС «ЦУБ» не реже одного раза в квартал, а также при каждом изменении параметров узлов безопасности, таких как: состав программного и (или) аппаратного обеспечения средств вычислительной техники, телекоммуникационного оборудования и виртуальных машин (путем ежедневного или событийного контроля изменений, а также иными способами, обеспечивающими уточнение инвентаризационной информации).

73. При необходимости изменения параметров узлов безопасности пользователь ГИС «ЦУБ» заблаговременно (за один рабочий день до момента внесения изменений) уведомляет оператора ГИС «ЦУБ» о планируемых изменениях.

74. Деятельность по инвентаризации включает в себя следующие этапы сбора сведений об узлах безопасности:

1) ФИО, должности и контактные данные лиц, ответственных за реагирование на КИ на узле безопасности, а также лиц, ответственных за принятие решений;

2) доменные имена и сетевые адреса узлов безопасности (средств вычислительной техники, телекоммуникационного оборудования, виртуальных машин и т. п.) в соответствии с системой имен и сетевой адресацией узла безопасности;

3) доменные имена и сетевые адреса компонентов узлов безопасности, доступные из информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет), в соответствии с системой имен и сетевой адресацией сети Интернет, а также сведения о протоколах (включая параметры транспортного уровня взаимодействия), по которым разрешен доступ к этим компонентам;

4) сведения о сегментации и топологии локальных вычислительных сетей;

5) перечень программного обеспечения (прикладного и системного), установленного на каждом узле безопасности;

6) параметры настройки программного и аппаратного обеспечения узлов безопасности, существенные с точки зрения обеспечения;

7) параметры настройки средств обеспечения ИБ.

75. Сбор и уточнение инвентаризационной информации выполняются оператором ГИС «ЦУБ» в пределах его зоны ответственности. Оператор ГИС «ЦУБ» предоставляет актуальную информацию по инвентаризации в НКЦКИ.

Глава 7. Порядок выявления уязвимостей узлов безопасности

76. Целью выявления уязвимостей узлов безопасности в процессе МКИ является определение недостатков в обеспечении безопасности узлов безопасности (включая уязвимости программного кода, ошибки в настройке, уязвимости архитектуры, ошибки в реализации мер защиты), которые могут использоваться нарушителем для проведения КА.

77. Выявление уязвимостей может выполняться следующими способами:

1) выявление известных уязвимостей сетевых служб, доступных для сетевого взаимодействия, с применением автоматизированных средств анализа защищенности (сетевое сканирование);

2) выявление известных уязвимостей программного обеспечения узлов безопасности путем анализа состава установленного программного обеспечения и обновлений безопасности с применением автоматизированных средств анализа защищенности (системное сканирование, исследование с использованием привилегированных учетных записей и (или) программных агентов), а также других средств защиты информации;

3) тестирование на проникновение в условиях, соответствующих условиям нарушителя, действующего со стороны сети Интернет и (или) со стороны информационных ресурсов, внешних по отношению к зоне ответственности узлов безопасности;

4) тестирование на проникновение в условиях, соответствующих условиям нарушителя, действующего со стороны информационных ресурсов, входящих в зону ответственности сегментов пользователя ГИС «ЦУБ»;

5) тестирование устойчивости к атакам типа «отказ в обслуживании»;

6) контроль устранения ранее выявленных уязвимостей и недостатков;

7) контроль выполнения требований безопасности информации, предъявляемых к контролируемой информационной системе;

8) анализ настроек программного и аппаратного обеспечения информационных систем, а также средств защиты информации;

9) анализ проектной, конструкторской и эксплуатационной документации информационных систем;

10) оценка соответствия применяемых мер защиты требованиям безопасности информации, предъявляемым к информационным ресурсам нормативными документами Российской Федерации и владельцев информационных ресурсов.

78. Оператор ГИС «ЦУБ» ежемесячно проводит сетевое и системное сканирование, анализ настроек узлов безопасности и направляет пользователю ГИС «ЦУБ» отчет об анализе уязвимостей, содержащий информацию об уязвимом программном обеспечении, критичности выявленных уязвимостей, рекомендуемых мерах по нейтрализации уязвимостей.

79. Пользователь ГИС «ЦУБ» анализирует предоставленный отчет об анализе уязвимостей и формирует план устранения уязвимостей в соответствии с их критичностью и возможностью эксплуатации для конкретных условий функционирования узлов безопасности. При необходимости пользователь ГИС «ЦУБ» привлекает оператора ГИС «ЦУБ» для уточнения описания выявленных уязвимостей и возможности их эксплуатации.

80. По результатам исполнения плана устранения уязвимостей, но не позднее двух недель с момента получения предоставленного отчета, пользователь ГИС «ЦУБ» направляет оператору ГИС «ЦУБ» отчет об устранении уязвимостей, который содержит информацию об узлах

безопасности, связанных с ним устраненных уязвимостях, а также информацию о методах, с помощью которых было произведено устранение уязвимости, среди которых:

1) обновление программного обеспечения;

2) отключение уязвимой функции/характеристики;

3) принятие компенсирующей меры, делающей невозможной эксплуатацию уязвимости;

4) анализ условий эксплуатации уязвимости и установление невозможности ее эксплуатации с учетом особенностей использования узла безопасности.

81. Оператор ГИС «ЦУБ» ежеквартально проводит контроль устранения ранее выявленных уязвимостей, оценку соответствия мер защиты, контроль выполнения требований ИБ путем сопоставления результатов из отчетов по анализам уязвимостей на начало и на конец квартала, отчета по устранению уязвимостей, предоставляемого пользователем ГИС «ЦУБ», а также перечня применяемых на информационной инфраструктуре пользователя ГИС «ЦУБ» мер защиты (в том числе средств защиты информации и их настроек).

82. По результатам указанных в пункте 81 настоящего регламента мероприятий оператор ГИС «ЦУБ» формирует отчет, содержащий перечень приоритетных уязвимостей для устранения и перечень рекомендуемых мер для реализации данного устранения и организации соответствия требованиям ИБ.

83. Оператор ГИС «ЦУБ» и пользователь ГИС «ЦУБ» не реже одного раза в год проводят тестирование на проникновение и нагрузочное тестирование. Данные мероприятия проводятся по отдельному согласованному плану, содержащему сроки проведения работ, перечень тестируемых узлов безопасности, информацию о методах тестирования и зонах ответственности.

84. Оператор ГИС «ЦУБ» осуществляет анализ проектной, конструкторской и эксплуатационной документации – перед вводом узла безопасности (информационной системы или ресурсов, состоящих из узлов безопасности) в эксплуатацию и при каждом существенном изменении состава программных или аппаратных средств узла безопасности (информационной системы или ресурсов, состоящих из узлов безопасности).

85. В случае внедрения или изменения компонентов информационной инфраструктуры или информационных систем, состоящих из компонентов информационной инфраструктуры, подпадающих под признаки узлов безопасности, пользователь ГИС «ЦУБ» передает оператору ГИС «ЦУБ» проектную, конструкторскую и эксплуатационную документацию для анализа. По результатам анализа оператор ГИС «ЦУБ» при необходимости формирует рекомендации по обеспечению защищенности указанных компонентов информационной инфраструктуры, информационных систем.

86. Оператор ГИС «ЦУБ» обеспечивает хранение результатов выявления уязвимостей в течение трех лет с момента проведения соответствующих исследований. По запросу НКЦКИ оператор ГИС «ЦУБ» предоставляет результаты выявления уязвимостей, проводившихся в отношении

запрашиваемого информационного ресурса в заданный промежуток времени, в пределах периода хранения результатов.

Глава 8. Порядок анализа угроз ИБ

87. Целью анализа угроз ИБ в процессе МКИ является определение возможных способов проведения КА на информационные системы, подключенные к ГИС «ЦУБ», с учетом особенностей, реализованных в них информационных технологий, состава их узлов безопасности и программного обеспечения, а также разработка предложений по противодействию КА, представляющим угрозу соответствующим информационным ресурсам.

88. Анализ угроз безопасности проводится оператором ГИС «ЦУБ» для информационных систем пользователя ГИС «ЦУБ», для которых организационно-распорядительной документацией на систему защиты информации определены параметры критичности конфиденциальности, целостности и доступности информации, а также проведено моделирование угроз. Для узлов безопасности, не имеющих формализованных параметров по защите информации, анализ угроз проводится по мере необходимости и выявлении явных уязвимостей и угроз безопасности узлу безопасности.

89. Оператор ГИС «ЦУБ» проводит анализ угроз безопасности на основе предоставляемых пользователем ГИС «ЦУБ» моделей угроз на информационные системы, инвентаризационной информации, а также результатов выявления уязвимостей. Анализ угроз безопасности включает в себя:

1) определение возможных угроз, связанных с КА на информационную систему, состоящую из узлов безопасности;

2) идентификацию уязвимостей, использование которых может позволить нарушителю выполнить КА;

3) определение способов проведения КА с использованием таких уязвимостей;

4) определение возможных признаков проведения таких КА, способов их обнаружения и мер реагирования на них;

5) определение возможных путей противодействия проведению таких КА;

6) выработку организационных и технических решений по противодействию КА.

90. На основе анализа угроз разрабатываются новые или уточняются существующие документы, включающие:

1) модели угроз безопасности информационных систем, подключенных к ГИС «ЦУБ»;

2) методические рекомендации по предупреждению, обнаружению и ликвидации последствий КА;

3) решающие правила средств обнаружения КА;

4) настройки средств обеспечения ИБ;

5) политики обеспечения ИБ;

6) нормативные правовые акты организации;

7) дополнительные требования по обеспечению ИБ для их включения

в технические задания на создание новых, доработку и обслуживание существующих информационных ресурсов;

8) правила корреляции событий, направленные на определение попыток реализации угроз, связанных с проведением КА;

9) инструкции для пользователей информационных ресурсов по выявлению признаков проведения типовых КА, порядку их обнаружения, действиям по ликвидации их последствий;

10) инструкции по действиям пользователей информационных ресурсов в случае возникновения КИ, связанных с КА;

11) требования к квалификации пользователей, необходимой для выполнения указанных выше норм и правил.

91. Оператор ГИС «ЦУБ» производит составление и актуализацию перечня угроз безопасности для узлов безопасности на основе проведенного анализа и информации, полученной от НКЦКИ.

92. В рамках взаимодействия между НКЦКИ и оператором ГИС «ЦУБ» возможен обмен информацией об актуальных угрозах информационной безопасности.

ПРИЛОЖЕНИЕ № 1
к регламенту эксплуатации
государственной информационной
системы Калининградской области
«Центр управления безопасностью»,
утвержденному приказом
Министерства цифровых технологий
и связи Калининградской области

от «23» апреля 2024 года № 92

ФОРМА

Соглашение
о подключении к государственной информационной системе
Калининградской области «Центр управления безопасностью»

г. Калининград «___» _____ 20__ г.

Министерство цифровых технологий и связи Калининградской области, в лице _____ (далее – Уполномоченный орган), действующего на основании_____, с одной стороны, Государственное казенное учреждение Калининградской области «Центр цифровых технологий» (далее соответственно – ГИС «ЦУБ», Оператор ГИС «ЦУБ»), в лице _____, действующего на основании _____, со второй стороны, и _____, (далее – Пользователь ГИС «ЦУБ»), в лице _____, действующего на основании _____, с третьей стороны, совместно именуемые «Стороны», в целях повышения уровня защищенности информационных ресурсов Пользователя ГИС «ЦУБ», посредством применения положений, установленных Регламентом по эксплуатации государственной информационной системы Калининградской области «Центр управления безопасностью» (далее – Регламент), утвержденным приказом Министерства цифровых технологий и связи Калининградской области от «____» _____ 2024 г. №___, заключили настоящее Соглашение (далее – Соглашение) о нижеследующем:

1. Предмет Соглашения

1.1. Предметом Соглашения является организация и осуществление взаимодействия Сторон по подключению компонентов информационной инфраструктуры Пользователя ГИС «ЦУБ» в процессе менеджмента инцидентов информационной безопасности, осуществляемого ведомственным

центром ГосСОПКА Оператора ГИС «ЦУБ».

1.2. Стороны при осуществлении взаимодействия в рамках Соглашения руководствуются Регламентом.

1.3. Заключение Сторонами Соглашения является необходимым условием для организации менеджмента инцидентов информационной безопасности.

2. Общие положения

2.1. Настоящим соглашением Пользователь ГИС «ЦУБ» подтверждает согласие с положениями Регламента.

2.2. Пользователь ГИС «ЦУБ» признаёт право Уполномоченного органа на внесение изменений и дополнений в Регламент и подтверждает обязательность признания соответствующих изменений и дополнений со дня уведомления его Уполномоченным органом о внесении изменений и дополнений в Регламент.

3. Права и обязанности Сторон

3.1. Уполномоченный орган обязуется:

3.1.1. Осуществлять организационное сопровождение и материально-техническое обеспечение ГИС «ЦУБ»;

3.1.2. Осуществлять контроль за исполнением Оператором ГИС «ЦУБ» обязанностей, установленных Регламентом;

3.1.3. В срок не позднее трёх рабочих дней с даты утверждения приказом Уполномоченного органа изменений и дополнений в Регламент уведомлять Пользователя ГИС «ЦУБ» о внесении изменений и дополнений в Регламент.

3.2. Оператор ГИС «ЦУБ» обязуется:

3.2.1. Обеспечивать функционирование ГИС «ЦУБ» в соответствии с требованиями Регламента;

3.2.2. Обеспечивать работоспособность и безопасность используемых Оператором ГИС «ЦУБ» программно-аппаратных и программных средств, необходимых для функционирования ГИС «ЦУБ» в соответствии с требованиями Регламента;

3.2.3. Обеспечивать предоставление информационной и методической поддержки Пользователя ГИС «ЦУБ» по вопросам исполнения Регламента;

3.2.4. По письменному представлению Уполномоченного органа производить отключение Пользователя ГИС «ЦУБ» от ГИС «ЦУБ»;

3.2.5. Обеспечивать строгое соблюдение установленного законодательством Российской Федерации порядка ограниченного доступа к отдельным видам информации, передаваемой в процессе взаимодействия Сторон, в том числе к персональным данным граждан;

3.2.6. Незамедлительно информировать Пользователя ГИС «ЦУБ» об обнаруженной временной организационной и (или) технической невозможности выполнения обязательств по Соглашению;

3.2.7. Устранять своими силами и за свой счет допущенные по своей вине недостатки или иные отступления от условий Соглашения;

3.2.8. Обеспечивать взаимодействие с Национальным координационным Центром по компьютерным инцидентам в рамках выполнения функций ведомственного центра государственной системы обнаружения и предотвращения компьютерных атак.

3.3. Пользователь ГИС «ЦУБ» обязуется:

3.3.1. Выполнять установленные Регламентом правила, а также иные требования, установленные в отношении своих информационных систем в соответствии с законодательством Российской Федерации;

3.3.2. В течение трёх рабочих дней с даты заключения настоящего Соглашения заполнить и направить Оператору ГИС «ЦУБ» заявку по форме, представленной в приложении № 2 к Регламенту.

3.3.3. Незамедлительно информировать Оператора ГИС «ЦУБ» об обнаруженной организационной и (или) технической невозможности выполнения обязательств по Соглашению;

3.3.4. Незамедлительно и в полном объёме информировать Оператора ГИС «ЦУБ» обо всех планируемых и (или) произведённых изменениях в составе и настройках информационной инфраструктуры, подключенной к ГИС «ЦУБ»;

3.3.5. Устранять своими силами и за свой счет допущенные по своей вине недостатки или иные отступления от условий Соглашения;

3.3.6. Обеспечивать достоверность и актуальность сведений, представляемых Оператору ГИС «ЦУБ», необходимых для исполнения Оператором ГИС «ЦУБ» предусмотренных Соглашением и Регламентом обязанностей;

3.3.7. В случае установления недостоверности переданных сведений обеспечивать их незамедлительное изменение (актуализацию);

3.3.8. Обеспечивать работоспособность и безопасность используемых ГИС «ЦУБ» программно-аппаратных и программных средств, необходимых для осуществления взаимодействия с Оператором ГИС «ЦУБ», в порядке установленном действующим законодательством;

3.3.9. Обеспечивать актуальность всех версий программного и аппаратного обеспечения, подключаемого к ГИС «ЦУБ»;

3.3.10. Обеспечивать строгое соблюдение установленного законодательством Российской Федерации порядка ограниченного доступа к отдельным видам информации, получаемой и передаваемой в процессе взаимодействия Сторон, в том числе к персональным данным граждан;

3.3.11. Не производить действия, направленные на нарушение информационной безопасности ГИС «ЦУБ».

3.4. Уполномоченный орган имеет право:

3.4.1. Своим приказом вносить изменения и дополнения в Регламент;

3.4.2. В одностороннем порядке принимать решение об отключении Пользователя ГИС «ЦУБ» от ГИС «ЦУБ» при нарушении Пользователем ГИС «ЦУБ» требований Регламента и (или) невыполнении взятых

по Соглашению обязательств.

3.5. Оператор ГИС «ЦУБ» имеет право:

3.5.1. Запрашивать у Пользователя ГИС «ЦУБ» сведения о выполнении установленных Регламентом требований;

3.5.2. Осуществлять текущий мониторинг соблюдения Пользователем ГИС «ЦУБ» установленных Регламентом правил и выполнения технических требований;

3.5.3. Предпринимать меры, направленные на предотвращение и устранение выявленных нарушений.

3.6. Пользователь ГИС «ЦУБ» имеет право:

3.6.1. На предоставление Оператором ГИС «ЦУБ» информационной и методической поддержки по вопросам исполнения Регламента;

3.6.2. По согласованию с Оператором ГИС «ЦУБ» и в соответствии с установленными Регламентом техническими требованиями модернизировать и обновлять компоненты информационной инфраструктуры в установленном порядке.

4. Ответственность Сторон

4.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по Соглашению в соответствии с требованиями законодательства Российской Федерации и условиями настоящего Соглашения.

4.2. Уполномоченный орган и Оператор ГИС «ЦУБ» не несут ответственности за:

4.2.1. Состояние используемых Пользователем ГИС «ЦУБ» каналов связи, средств и систем обеспечения информационного обмена, межсетевого взаимодействия и защиты информации, соответствие действующим требованиям мероприятий по технической защите информации в информационных системах Пользователя ГИС «ЦУБ»;

4.2.2. Аварии, сбои или перебои в обслуживании используемых Пользователем ГИС «ЦУБ» программных, программно-аппаратных компонентах информационных систем, средств и систем обеспечения информационного обмена;

4.2.3. Ущерб, понесенный Пользователем ГИС «ЦУБ» в результате нарушения им Соглашения и Регламента.

4.3. Пользователь ГИС «ЦУБ» не несет ответственности за ущерб, понесенный Уполномоченным органом и Оператором ГИС «ЦУБ», иными Участниками, при отсутствии вины Пользователя ГИС «ЦУБ».

4.4. Уполномоченный орган, Оператор ГИС «ЦУБ» и пользователь ГИС «ЦУБ» не несут ответственности за неисполнение или ненадлежащее исполнение обязательств, принятых на себя в соответствии с Соглашением, если надлежащее исполнение оказалось невозможным вследствие наступления обстоятельств непреодолимой силы.

4.5. Для целей Соглашения термин «непреодолимая сила» означает

обстоятельства, предусмотренные пунктом 3 статьи 401 Гражданского кодекса Российской Федерации.

4.6. Уполномоченный орган, Оператор ГИС «ЦУБ» и пользователь ГИС «ЦУБ» в случае невозможности исполнения своих обязательств по причине наступления обстоятельств непреодолимой силы, должны предпринять все возможные действия для извещения другой Стороны о наступлении таких обстоятельств.

4.7. Исполнение обязательств возобновляется немедленно после прекращения действия обстоятельств непреодолимой силы.

5. Приостановление процесса взаимодействия

5.1. Процесс взаимодействия Пользователя ГИС «ЦУБ с ГИС «ЦУБ» может быть прекращен в случаях:

5.1.1. Нарушения Пользователем ГИС «ЦУБ» установленных Регламентом правил и технических требований;

5.1.2. Выявления фактов деструктивных действий Пользователя ГИС «ЦУБ» по отношению к ГИС «ЦУБ».

5.2. В случае выявления признаков нарушений, предусмотренных п. 5.1 Соглашения, Оператор ГИС «ЦУБ» в срок, не превышающий трех рабочих дней, направляет Пользователю ГИС «ЦУБ» и Уполномоченному органу уведомление о выявленных нарушениях.

5.3. Отключение Пользователя ГИС «ЦУБ» от взаимодействия с ГИС «ЦУБ» производится Оператором ГИС «ЦУБ» немедленно после уведомления Уполномоченного органа о решении по отключению.

6. Порядок разрешения споров

6.1. Все споры или разногласия, возникающие между Сторонами по Соглашению или в связи с ним, разрешаются путем переговоров и консультаций между Сторонами.

6.2. В случае если спор или разногласия не могут быть разрешены путем переговоров и (или) консультаций между Сторонами, создается экспертная комиссия.

6.3. Состав экспертной комиссии формируется из равного количества представителей каждой из Сторон. В состав экспертной комиссии по согласованию с Уполномоченным органом и Оператором ГИС «ЦУБ» также могут включаться эксперты – представители независимых органов и (или) организаций.

6.4. Дата, место и время начала заседания экспертной комиссии согласовываются всеми Сторонами.

6.5. В случае неявки на заседание экспертной комиссии представителей одной из Сторон заседание проводится без их участия. Об отсутствии представителей Стороны составляется акт, который подписывается всеми присутствующими участниками экспертной комиссии.

6.6. Решение, принятое на заседании экспертной комиссии, оформляется соответствующим протоколом.

6.7. Переговорный порядок урегулирования споров и разногласий не исключает права каждой из Сторон на разрешение споров в судебном порядке в соответствии с законодательством Российской Федерации. Стороны обязуются возникающие споры разрешать в Арбитражном суде Калининградской области.

7. Заключительные положения

7.1. Ответственными за организационно-техническое обеспечение реализации Соглашения являются:

от Уполномоченного органа – _____;

от Оператора ГИС «ЦУБ» – _____;

от Пользователя ГИС «ЦУБ» – _____.

7.2. Соглашение вступает в силу с момента его подписания, действует до _____ 20___ г. и автоматически продлевается на каждый последующий год, если ни одна из Сторон за 10 (десять) рабочих дней до истечения действующего срока Соглашения письменно не заявит о своем намерении расторгнуть данное Соглашение.

7.3. В случае изменения наименования, адреса места нахождения или других реквизитов одной из Сторон, Сторона письменно извещает об этом другую Сторону в течение трех рабочих дней со дня такого изменения.

7.4. В случае необходимости изменения данных, представленных Пользователем ГИС «ЦУБ в заявках на подключение к ГИС «ЦУБ», Пользователь ГИС «ЦУБ» письменно извещает об этом Оператора ГИС «ЦУБ» не менее чем за пять рабочих дней до планируемой даты такого изменения.

7.5. Дополнения и изменения Соглашения, принимаемые по предложениям Сторон, оформляются в письменной форме в виде дополнительных соглашений, которые становятся неотъемлемой частью Соглашения с момента их подписания Сторонами.

7.6. Соглашение в течение срока действия может быть расторгнуто по инициативе любой из Сторон, при этом она должна письменно уведомить другую Сторону не менее чем за один календарный месяц до предполагаемой даты прекращения действия Соглашения.

7.7. Расторжение Соглашения возможно в случаях и порядке, установленных законодательством Российской Федерации.

7.8. Соглашение составлено в трех экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

8. Адрес места нахождения, реквизиты и подписи Сторон

Министерство цифровых технологий и связи Калининградской области	**Оператор ГИС «ЦУБ»**	**Пользователь ГИС «ЦУБ»**
236007 г. Калининград, ул. Дмитрия Донского, 1 ИНН 3906227616 КПП 390601001 УФК по Калининградской области л/с 03352P08110 Отделение Калининград, г. Калининград, р/с 40201810700000000005 БИК 042748001	236007, г. Калининград, ул. Дмитрия Донского, 1 ИНН 3906361562 КПП: 390601001 ОГРН: 1173926028704 Банковские реквизиты: р/с 40102810545370000028; БИК 012748051; к/с 03100643000000013500; банк получателя: Отделение Калининград Банка России//УФК по Калининградской области г. Калининград; получатель: Министерство финансов Калининградской области (ГКУ КО «ЦЦТ» л/с 04352J03460)	
_____/_____ _/ М.п.	_____/_____/ М.п.	_____/_____/ М.п.

ПРИЛОЖЕНИЕ № 2
к регламенту эксплуатации
государственной информационной
системы Калининградской области
«Центр управления безопасностью»,
утвержденному приказом Министерства
цифровых технологий и связи
Калининградской области

от «23» апреля 2024 года № 92

ФОРМА

Оператору государственной
информационной системы
Калининградской области
«Центр управления безопасностью»

З А Я В К А
на подключение к государственной информационной системе Калининградской области «Центр управления безопасностью» - ведомственному центру ГосСОПКА

Прошу подключить компоненты информационной инфраструктуры _____[1]
для организации процесса менеджмента инцидентов информационной безопасности.

Приложение:
1. Карточка организации

_____ _____ _____
(должность руководителя) (подпись) (расшифровка подписи)

М.П.

[1] Полное наименование Пользователя ГИС «ЦУБ» в родительном падеже.

Приложение
к заявке на подключение
к ГИС «ЦУБ» в части менеджмента
инцидентов информационной
безопасности

Карточка
организации, подключаемой к процессу менеджмента инцидентов информационной безопасности ГИС «ЦУБ»

1	Наименование организации	
2	Адрес(а) расположения информационной инфраструктуры	
3	Наименование провайдера, оказывающего услуги связи	
4	Топологические схемы информационной инфраструктуры	
5	Наличие домен-контроллера (IP, FQDN)	
6	Наличие почтового сервера (IP, доменное имя)	
7	Наличие информационных систем с формализованной системой защиты информации (ГИС/ ИСПДн/ КИИ)	
8	Перечень доменных имен	
9	Перечень ресурсов, маршрутизируемых в сети Интернет (IP – доменное имя)	
10	Сведения о сегментации и топологии локальных вычислительных сетей, правилах маршрутизации и коммутации, настройках средств межсетевого экранирования	
11	Перечень VLan организации (номер VLan – назначение)	
12	Перечень уникальных средств вычислительной техники (включая любое сетевое оборудование, например ИБП, сетевые МФУ, оборудование IP-телефонии)	
13	Перечень уникальных моделей телекоммуникационного оборудования с указанием количества	
14	Перечень уникального используемого общесистемного программного обеспечения с указанием количества и версий	
15	Перечень уникального используемого прикладного программного обеспечения с указанием количества и версий	
16	Перечень уникальных средств защиты, установленных на рабочих станциях пользователей	

17	Перечень уникальных средств защиты, установленных на серверном оборудовании	
18	Перечень средств криптографической защиты информации, реализующих функции защиты каналов связи (указать производителя и модель)	
19	Сведения о подключении информационных ресурсов к другим объектам информационной инфраструктуры (перечень сопряженных сетей с указанием владельцев сетей и адресного пространства)	
20	Правила парольной политики, принятые в организации*	
21	Правила проведения инвентаризации*	
22	Модель угроз и модель нарушителя (злоумышленника)*	
23	Правила установки обновлений*	
24	Контактные данные лица, ответственного за защиту информации в организации (Ф.И.О., должность, контактный телефон, электронная почта)	

Пользователь ГИС «ЦУБ»
Должность, ФИО Дата

*При наличии прикладывается к заявке

ПРИЛОЖЕНИЕ № 3
к регламенту эксплуатации
государственной информационной
системы Калининградской области
«Центр управления безопасностью»,
утвержденному приказом Министерства
цифровых технологий и связи
Калининградской области

от «23» апреля 2024 года № 92

ФОРМА

Паспорт узла безопасности

1	Производитель оборудования, программного обеспечения	
2	Тип узла безопасности (нужное подчеркнуть)	Физический сервер/ виртуальная машина /сетевое оборудование / программное обеспечение
3	Имя узла безопасности	
4	Входит в состав ГИС/ИСПДн/ КИИ (указать наименование)	
5	Наименование и версия системного программного обеспечения	
6	Краткое описание выполняемых функций	
7	Способ подключения к узлу безопасности пользователями (нужное подчеркнуть)	Локально, порт-протокол
8	Адрес расположения	Площадка, наименование организации, CDTO – при наличии
9	IP-адрес	
10	Параметры сети устройства (IP-адрес шлюза, VLAN)	
11	Имеет ли узел безопасности выход в сеть «Интернет»?	Да / Нет
12	Список ресурсов сети Интернет, необходимых для функционирования узла безопасности (заполняется заблаговременно)	
13	Влияние на иные процессы в случае выхода из строя/некорректной работы (опционально)	
14	Наличие технологических связей с другими узлами / группами узлов (имя узла, тип, технология соединения, IP адрес узла, используемые для соединения порты)	
15	Перечень административных учетных записей с их правами на данном узле	

16	Наименование учетной записи с правом администратора для подключения к мониторингу (опционально)	
17	Перечень прикладного программного обеспечения, установленного на узле и выполняющего основные функции узла (наименование, версия)	
18	Перечень вспомогательного программного обеспечения (наименование, версия)	
19	Параметры настройки программного и аппаратного обеспечения информационного ресурса, существенные с точки зрения обеспечения безопасности информации	
20	Параметры настройки средств обеспечения информационной безопасности	
21	Контактные данные ответственного за реагирование на компьютерные инциденты	Ф.И.О., должность, эл. адрес, контактный номер телефона
22	Контактные данные ответственного за принятие решений	Ф.И.О., должность, эл. адрес, контактный номер телефона

Оператор узла ЕИТС/ Пользователь ГИС «ЦУБ»
Должность, ФИО Дата

Оператор ГИС «ЦУБ»
Должность, ФИО Дата