МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ И СВЯЗИ КАЛИНИНГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

15 июня 2021 г. № 242

Калининград

Об утверждении Временного регламента взаимодействия между оператором и администратором информационной безопасности единой информационной телекоммуникационной сети Правительства Калининградской области, а также уполномоченным органом

В соответствии с постановлением Правительства Калининградской области от 04 июня 2018 года № 301 «Об утверждении положения о единой информационно-телекоммуникационной сети Правительства Калининградской области», в целях совершенствования основных принципов создания, использования и развития единой информационно-телекоммуникационной сети Правительства Калининградской области, обеспечения единства и информационной безопасности данной сети и эффективности использования средств областного бюджета, выделяемых на услуги связи, п р и к а з ы в а ю:

1. Утвердить Временный регламент взаимодействия между оператором и администратором информационной безопасности единой информационной телекоммуникационной сети Правительства Калининградской области, а также уполномоченным органом (далее – Регламент) согласно приложению к настоящему приказу.

2. Руководителям подведомственных Министерству цифровых технологий и связи Калининградской области государственного автономного учреждения Калининградской области «Калининградский государственный научно-исследовательский центр информационной и технической

безопасности» (далее – КГ НИЦ) и государственного бюджетного учреждения Калининградской области «Центр цифровых технологий» (далее – ГБУ КО «ЦЦТ»):

- назначить ответственных по направлениям деятельности во исполнение настоящего приказа из числа сотрудников учреждений;

- в срок до 29 июня 2021 года осуществить группировку компонентов единой информационно-телекоммуникационной сети Правительства Калининградской области (далее – ЕИТС) по функциональным категориям с последующей приоритезацией категорий по 3 уровням отнесения компонентов ЕИТС к узлам безопасности – «высокий», «средний» или «низкий» в соответствии с параметрами, изложенными в Регламенте;

3. ГБУ КО «ЦЦТ», при необходимости с привлечением КГ НИЦ осуществить:

- в срок до 05 июля 2021 года формирование списка компонентов ЕИТС с приоритетом отнесения к узлам безопасности «высокий»;

- в срок до 16 августа 2021 года заполнение и передачу в КГ НИЦ паспортов узлов безопасности на компоненты ЕИТС с приоритетом отнесения к узлам безопасности «высокий»;

- в срок до 23 августа 2021 года формирование списка компонентов ЕИТС с приоритетом отнесения к узлам безопасности «средний»;

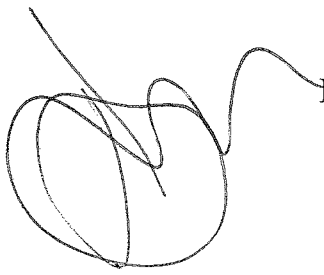
- в срок до 04 октября 2021 года заполнение и передачу в КГ НИЦ паспортов узлов безопасности на компоненты ЕИТС с приоритетом отнесения к узлам безопасности «средний»;

- в срок до 15 октября 2021 года формирование списка компонентов ЕИТС с приоритетом отнесения к узлам безопасности «низкий»;

- в срок до 29 ноября 2021 года заполнение и передачу в КГ НИЦ паспортов узлов безопасности на компоненты ЕИТС с приоритетом отнесения к узлам безопасности «низкий».

4. КГ НИЦ по выполнению пункта 2 настоящего Приказа разработать и организовать ведение плана приоритетного отнесения существующих компонентов ЕИТС к узлам безопасности, и, в соответствии с разработанным планом, положениями Регламента и имеющимися техническими и технологическими возможностями государственной информационной системы «Центр управления безопасности», обеспечить включение компонентов ЕИТС в процесс мониторинга инцидентов информационной безопасности.

5. Приказ вступает в силу со дня его официального опубликования.

Министр  В.В. Рыскаль

ПРИЛОЖЕНИЕ
к приказу Министерства цифровых
технологий и связи
Калининградской области
от 15 июня 2021 г. № 242

ВРЕМЕННЫЙ РЕГЛАМЕНТ
взаимодействия между оператором и администратором информационной безопасности единой информационной телекоммуникационной сети Правительства Калининградской области, а также уполномоченным органом

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область действия

1.1.1. Настоящий временный регламент определяет процесс взаимодействия участников в ходе мониторинга компьютерных инцидентов информационной безопасности (далее – инциденты ИБ), а также локализации и ликвидации последствий инцидентов ИБ.

1.1.2. К участникам в рамках настоящего временного регламента относятся:

- оператор единой информационной телекоммуникационной сети Правительства Калининградской области (далее – ЕИТС);

- администратор информационной безопасности ЕИТС;

- уполномоченный орган;

- владелец (функциональный заказчик) информационной системы, сервиса, ресурса или оборудования, размещаемого в ЕИТС.

1.1.3. Настоящий Регламент устанавливает:

- порядок включения узла безопасности в процесс мониторинга инцидентов ИБ;

- порядок оперативного уведомления участников информационного взаимодействия об изменениях в ЕИТС;

- порядок выявления и регистрации инцидентов ИБ;

- порядок реагирования на инцидент ИБ и ликвидации последствий;

- порядок закрытия инцидента ИБ.

1.1.4. Ознакомление лиц, участвующих в процессе мониторинга инцидентов ИБ в ЕИТС, с настоящим Регламентом является обязательным.

1.1.5. Мониторинг инцидентов ИБ организуется для обеспечения конфиденциальности, целостности и доступности информации, обрабатываемой узлами ИБ ЕИТС.

1.1.6. Мониторинг инцидентов ИБ реализуется в рамках функций государственной информационной системы «Центр управления безопасностью» (далее – ГИС «ЦУБ»), на основании постановления Правительства Калининградской области от 10.11.2020 № 804 «О создании государственной информационной системы Калининградской области «Центр управления безопасностью».

1.1.7. Настоящий временный регламент подлежит исполнению в рамках опытного взаимодействия участников до момента принятия ГИС «ЦУБ» в промышленную эксплуатацию.

1.2. Участники взаимодействия и каналы взаимодействия

1.2.1. Уполномоченный орган – Министерство цифровых технологий и связи Калининградской области.

1.2.2. Оператор ЕИТС – Государственное бюджетное учреждение Калининградской области «Центр цифровых технологий» (далее – ЦЦТ).

1.2.3. Администратор информационной безопасности ЕИТС (далее администратор ИБ ЕИТС) – Государственное автономное учреждение Калининградской области «Калининградский государственный научно-исследовательский центр информационной и технической безопасности» (далее – КГ НИЦ) – оператор ГИС «ЦУБ».

1.2.4. Взаимодействие между участниками в рамках настоящего регламента организуется по следующими способами:

- с Администратором ИБ ЕИТС: по электронной почте soc@kgnic.ru, через единую систему электронного документооборота Правительства Калининградской области;

- оператором ЕИТС: через систему технической поддержки https://hd.gov39.ru, по электронной почте helpdesk@gov39.ru, через единую систему электронного документооборота Правительства Калининградской области;

- с Уполномоченным органом: по электронной почте inform@gov39.ru, через единую систему электронного документооборота Правительства Калининградской области.

1.3.Термины, сокращения и определения

В настоящем Регламенте используются следующие термины и определения:

ИБ	Информационная безопасность
ЕИТС	Единая информационно-телекоммуникационная сеть Правительства Калининградской области, созданная на основании постановления Правительства Калининградской области от 04.06.2018 № 301
НПА	Нормативные правовые акты
Инцидент ИБ	Появление одного или нескольких событий ИБ, которые могут свидетельствовать о целенаправленном воздействии программных и (или) программно-аппаратных средств на узлы безопасности или же иные объекты, используемые для организации взаимодействия таких узлов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации
Карточка инцидента ИБ	Информационный сервис или информационный реестр, содержащий информацию о подтвержденных инцидентах ИБ
Ответственный за устранение	Определенная организация, в полномочиях которой находятся операции по устранению инцидента ИБ

инцидента ИБ	
Система анализа событий безопасности	Система, позволяющая на основе правил определить соответствие порядка и качества событий безопасности инциденту ИБ
Событие безопасности	Идентифицированное возникновение определенного состояния системы, сервиса или сети, указывающее (прямо или косвенно) на возможное нарушение политики информационной безопасности, отказ защитных мер или возникновение неизвестной ранее ситуации, которая может иметь отношение к информационной безопасности
Процесс мониторинга инцидентов ИБ	Процесс, в ходе которого выполняются выявление, учет, регистрация, анализ, информирование, реагирование устранение и закрытие инцидентов ИБ узлов безопасности ЕИТС
Компонент ЕИТС	Программное, программно-аппаратное средство, выполняющее функции по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передачи (распространению, предоставлению доступа), блокированию, удалению, уничтожению данных в составе ЕИТС
Узел безопасности	Включенное в ЕИТС управляемое (активное) программное, программно-аппаратное средство из реестра компонентов ЕИТС, выполняющее функции по обработке, хранению, передаче, вводу/выводу информации, или же иные функции, обеспечивающие функционирование таких средств, информация о котором особым образом формализована с целью включения в процесс мониторинга инцидентов ИБ Перечень узлов безопасности определяется администратором защищенной сети ЕИТС и оператором ЕИТС и в первую очередь включает: - серверное оборудование и системы хранения данных; - виртуальные машины; - активное сетевое оборудование; - серверное общесистемное и специализированное программное обеспечение, базы данных

1.4. Нормативные ссылки

Нормативные правовые акты и руководящие документы, на основании которых разработан настоящий временный регламент:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- постановление Правительства Калининградской области от 04 июня 2018 года № 301 «Об утверждении положения о единой информационно-телекоммуникационной сети Правительства Калининградской области»;

- постановление Правительства Калининградской области от 10 ноября 2020 года № 804 «О создании государственной информационной системы Калининградской области «Центр управления безопасностью»;

- приказ Министерства цифровых технологий и связи Калининградской области от 18 июня 2020 года № 252 «Об осуществлении полномочий администратора защищенной сети единой информационно-телекоммуникационной сети Правительства Калининградской области»;

- приказ Министерства цифровых технологий и связи Калининградской области от 27 мая 2020 года № 216 «Об операторе единой информационно-телекоммуникационной сети Правительства Калининградской области»;

- ГОСТ Р ИСО/МЭК ТО 18044-2007 «Менеджмент инцидентов информационной безопасности».

II. ОПРЕДЕЛЕНИЕ УЗЛОВ БЕЗОПАСНОСТИ И ПОДДЕРЖАНИЕ ИНФОРМАЦИИ О НИХ В АКТУАЛЬНОМ СОСТОЯНИИ

2.1. Идентификация узла, как узла безопасности и включение узла безопасности в процесс мониторинга инцидентов ИБ

2.1.1. К узлам ЕИТС относятся:

- серверное оборудование и системы хранения данных;

- активное сетевое оборудование;

- автоматизированные рабочие места пользователей;

- активное периферийное оборудование;

- общесистемное и специализированное программное обеспечение.

2.1.2. Оператором ЕИТС осуществляется ведение реестра компонентов ЕИТС, при этом на каждый компонент из реестра ЕИТС, отнесенный к узлу безопасности, формируется паспорт узла безопасности.

2.1.3. Отнесение компонента ЕИТС к узлу безопасности и его дальнейшее подключение к процессу мониторинга осуществляется в порядке приоритета, обусловленного:

- критичностью выполняемых компонентом ЕИТС функций в приложении к свойствам безопасности обрабатываемой информации (конфиденциальность, целостность, доступность) в соответствии с требованиями нормативных документов по защите информации;

- влиянием компонента ЕИТС на другие компоненты ЕИТС (на их возможность выполнять свои функции в штатном режиме);

- возможным репутационным ущербам (в случае публичных сервисов).

2.1.4. Устанавливаются 3 уровня приоритета отнесения компонентов 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):

Высокий	**Средний**	**Низкий**
Отказ в обслуживании компонента ЕИТС может повлиять на работоспособность более 50 других компонентов ЕИТС	Отказ в обслуживании компонента ЕИТС может повлиять на работоспособность более 10, но менее 50 других компонентов ЕИТС	Отказ в обслуживании компонента ЕИТС может повлиять на работоспособность менее 10 других компонентов ЕИТС
Компрометация компонента ЕИТС может привести к компрометации других компонентов ЕИТС	Компрометация компонента ЕИТС может создать предпосылки к компрометации других компонентов ЕИТС	Компрометация компонента ЕИТС не может создать предпосылки к компрометации других компонентов ЕИТС, но к свойствам информации,

		обрабатываемой на компоненте ЕИТС, предъявляются требования по обеспечению либо, конфиденциальности, либо целостности, либо доступности
Компрометация компонента ЕИТС может нанести репутационный ущерб структурным подразделениям Правительства или органам исполнительной власти Калининградской области	Компрометация компонента ЕИТС может нанести репутационный ущерб подведомственному учреждению органа исполнительной власти Калининградской области	Компрометация компонента ЕИТС может нанести репутационный ущерб муниципальному образованию или подведомственному учреждению муниципального образования Калининградской области

Оператор ЕИТС и администратор ИБ ЕИТС в рамках совместной рабочей группы, образованной приказом уполномоченного органа, разрабатывают план приоритетного отнесения существующих компонентов ЕИТС к узлам безопасности для включения их в процесс мониторинга.

Указанный план должен содержать следующие мероприятия:

- группировка компонентов ЕИТС по категориям, соответствующим 3 уровням приоритета отнесения компонентов ЕИТС к узлам безопасности – «высокий», «средний» или «низкий»;

- формирование списка компонентов ЕИТС с приоритетом отнесения к узлам безопасности «высокий», «средний», «низкий»;

- заполнение паспортов узлов безопасности на компоненты ЕИТС с приоритетом отнесения к узлам безопасности «высокий», «средний», «низкий»;

2.1.5. В случае выявления существующих или внедрения новых компонентов ЕИТС, не включенных в план приоритетного отнесения существующих компонентов ЕИТС к узлам безопасности (в соответствии с п. 2.1.4 Регламента), подлежащих с учетом критериев отнесению к узлам безопасности, такие компоненты подлежат приоритезации и включению в указанный план в соответствии п. 2.1.4 настоящего Регламента.

2.1.6. Согласно плану отнесения существующих компонентов ЕИТС к узлам безопасности, оператор ЕИТС заносит информацию в паспорт узла безопасности, согласно Приложению 1 к настоящему временному регламенту. Паспорт направляется администратору ИБ ЕИТС, с фиксацией данных о получении Паспорта. Копия паспорта также направляется владельцу (функциональному заказчику) оборудования, системы или сервиса ЕИТС, с фиксацией факта получения. Администратор ИБ ЕИТС – идентифицирует компонент ЕИТС, как узел безопасности ЕИТС и запускает процесс его мониторинга.

2.1.7. С получением паспорта, администратор ИБ ЕИТС в срок не более, чем два рабочих дня, рассматривает и принимает паспорт узла безопасности для включения в процесс мониторинга инцидентов ИБ, или же направляет в адрес оператора ЕИТС уточняющий запрос, с целью установления параметров, недостающих для организации процесса мониторинга инцидентов ИБ.

2.1.8. Оператор ЕИТС с получением уточняющего запроса в течение двух рабочих дней, по согласованию, при необходимости, с владельцем (функциональным заказчиком) компонента ЕИТС, формирует ответ, содержащий информацию, необходимую для включения узла безопасности в процесс мониторинга инцидентов ИБ.

2.1.9. В случае невозможности включения узла безопасности администратор ИБ ЕИТС в течение двух рабочих дней с момента получения паспорта узла безопасности уведомляет оператора ЕИТС, уполномоченный орган и владельца (функционального заказчика) с указанием объективных причин.

2.1.10. В случае, если план отнесения существующих компонентов ЕИТС к узлам безопасности выполнен и включение указанных в плане компонентов произведено в полном объеме, при выявлении компонентов, не рассмотренных во время планирования отнесения компонентов ЕИТС к узлам безопасности, и отнесение которых к узлам безопасности необходимо с точки зрения

критериев отнесения, или же при внедрении новых компонентов ЕИТС, оператор ЕИТС производит паспортизацию узла безопасности без проведения приоритезации.

2.2. Учет и актуализация информации об узлах безопасности

2.2.1. Оператор ЕИТС осуществляет ведение реестра компонентов ЕИТС, в котором учитывается информация, необходимая для включения узлов безопасности в процесс мониторинга инцидентов ИБ, обеспечивает его выгрузку в специальный информационный ресурс, доступ к которому предоставлен оператору ЕИТС, администратору ИБ ЕИТС, уполномоченному органу.

Статус включения узлов безопасности в процесс мониторинга инцидентов ИБ в реестре компонентов ЕИТС устанавливает администратор ИБ ЕИТС.

2.2.2. В случае выявления администратором ИБ ЕИТС компонента ЕИТС, параметры которого подпадают под критерии отнесения к узлам безопасности, но не отнесенного к узлу безопасности, администратор ИБ ЕИТС сообщает об этом в Систему технической поддержки оператора ЕИТС. Оператор ЕИТС в течении двух рабочих часов локализует неучтённый компонент ЕИТС и направляет в адрес администратора ИБ ЕИТС информацию о неучтённом узле и предполагаемом уровне приоритета для его согласования и последующего описания, а также определения сроков его паспортизации.

2.2.3. С целью систематизации информации о ресурсах ЕИТС, включаемых в процесс мониторинга инцидентов ИБ, оператор ЕИТС разрабатывает структурную схему ЕИТС и отражает на ней все существующие и вновь включаемые в процесс мониторинга узлы ЕИТС. Указанная схема поддерживается в актуальном состоянии оператором ЕИТС и передается администратору ИБ ЕИТС при внесении изменений в указанную схему или же по запросу.

2.2.4. В случае необходимости внесения изменений в параметры функционирования узла безопасности, включенного в процесс мониторинга инцидентов ИБ, или же иного оборудования влияющего на процесс

его функционирования, оператор ЕИТС заблаговременно (не менее одного рабочего дня) уведомляет администратора ИБ ЕИТС о планируемых изменениях параметров, а также о результатах внесения указанных изменений. При этом оператор ЕИТС в течение двух рабочих дней заполняет и направляет в адрес администратора ИБ ЕИТС и владельца (функционального заказчика) обновленную анкету узла безопасности в части произведенных изменений. Оператор ЕИТС при внесении любых изменений обеспечивает доступность администратору ИБ ЕИТС узлов безопасности, переданных в процесс мониторинга инцидентов ИБ.

2.2.5. В случае, если общесистемные настройки узла безопасности не соответствуют требуемым для организации процесса мониторинга инцидента ИБ, администратор ИБ ЕИТС передает перечень таких настроек оператору ЕИТС. Оператор ЕИТС осуществляет новые настройки в течение двух рабочих дней или в течение одного рабочего дня запрашивает уточняющую информацию, или дает мотивированный отказ. О всех выполняемых действиях с настройкой параметров компоненты ЕИТС оператор ЕИТС уведомляет уполномоченный орган, администратора ИБ ЕИТС, владельца (функционального заказчика).

2.2.6. В случае, если настройки, необходимые для мониторинга ИБ, приводят к нарушению работоспособности компонента ЕИТС, оператор ЕИТС информирует администратора ИБ ЕИТС. Администратор ИБ ЕИТС в максимально кратчайший срок принимает меры по изменению параметров для восстановления работоспособности компонента ЕИТС, или сообщает оператору ЕИТС список настроек, которые необходимо внести на компонент ЕИТС для восстановления работоспособности компонента ЕИТС.

2.2.7. В случае отсутствия необходимости в осуществлении процесса мониторинга в отношении отдельных подключенных узлов безопасности, или же в связи с перераспределением вычислительных или технологических мощностей администратора ИБ ЕИТС для включения в процесс мониторинга

более критичных узлов безопасности, оператор ЕИТС направляет согласованную с уполномоченным органом заявку администратору ИБ ЕИТС об исключении узлов безопасности из процесса мониторинга. Оператор ЕИТС вносит в реестр компонентов ЕИТС информацию об исключении соответствующих узлов безопасности из процесса мониторинга.

2.2.8. При получении заявки, описанной в п.2.2.8 настоящего Регламента, администратор ИБ ЕИТС производит необходимые операции по исключению узлов безопасности из процесса мониторинга в срок, не превышающий один рабочий день. В случае отсутствия автоматизированного сервиса (системы) по ведению реестра компонентов ЕИТС, администратор ИБ ЕИТС вносит информацию в реестр узлов безопасности об исключении узлов из процесса мониторинга инцидентов ИБ.

III. ОБРАБОТКА ИНЦИДЕНТА ИБ

3.1. Этапы обработки инцидента ИБ

Процесс мониторинга инцидентов ИБ состоит из следующих этапов:

1. Выявление инцидента ИБ: анализ событий безопасности, поступающих от источников выявления инцидента ИБ, определение инцидента ИБ по заданным правилам, его регистрация и классификация, создание карточки инцидента ИБ;

2. Анализ инцидента ИБ: подтверждение инцидента ИБ, оценка критичности (приоритезация устранения инцидента ИБ), выявление причин и источника возникновения, выявление участвующего в инциденте ИБ узла безопасности ЕИТС, запрос необходимых сведений, формирование алгоритма устранения, определение исполнителя, ответственного за устранение, фиксация данных сведений в карточке инцидента ИБ;

3. Устранение инцидента ИБ: исполнение алгоритма устранения или локализации, в том числе устранение причин, блокирование источника возникновения последствий инцидента ИБ;

4. Контроль устранения инцидента ИБ: анализ событий безопасности, поступающих от источника, зафиксировавшего инцидент ИБ и другим косвенным признакам, на предмет соответствия параметрам инцидента ИБ;

5. Закрытие инцидента ИБ: перевод статуса инцидента ИБ в статус «закрытый», фиксация сведений о принятых мерах для устранения инцидента ИБ, формирование связи инцидента ИБ с узлом безопасности в реестре узлов безопасности, уведомление уполномоченного органа.

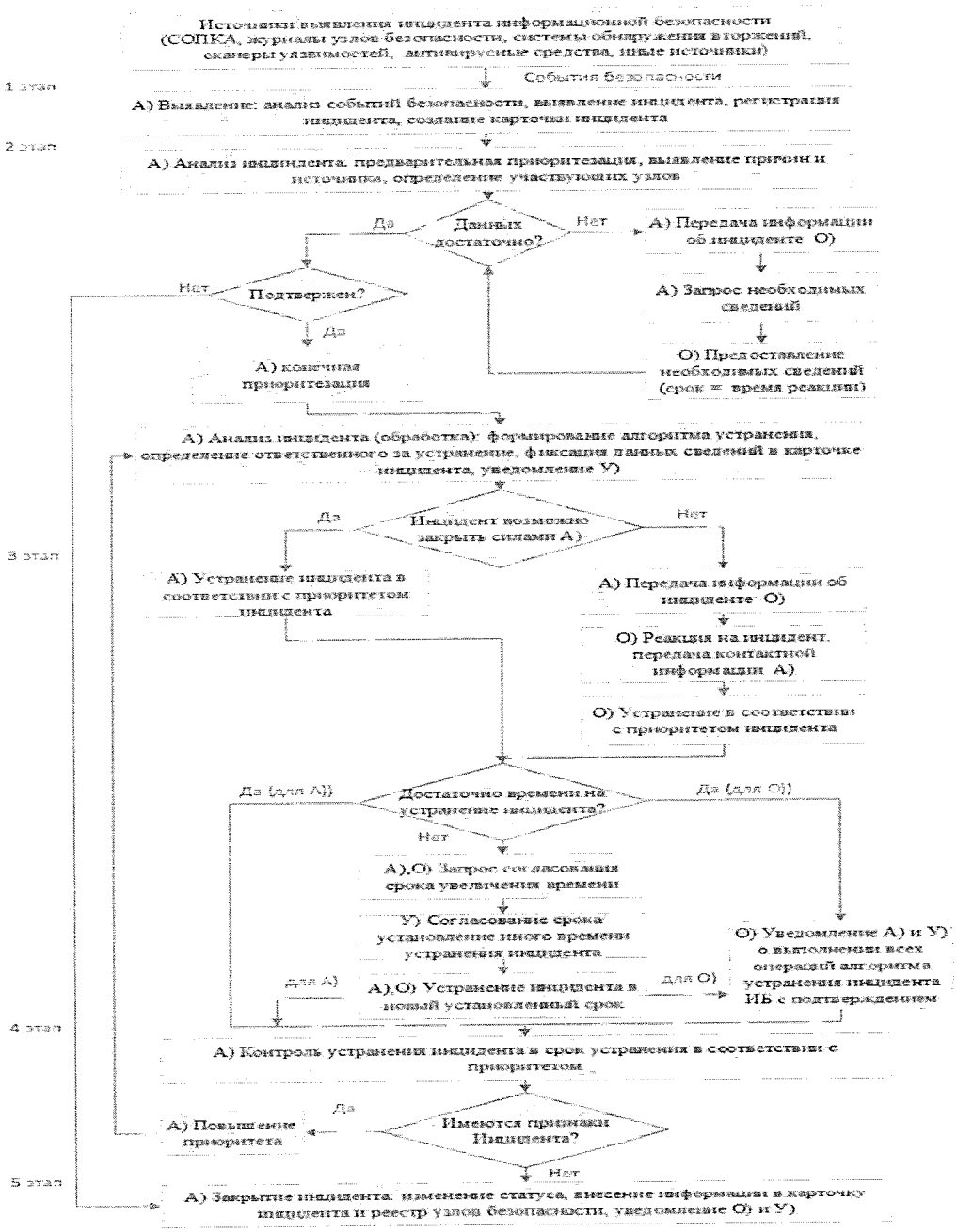


Рис. 1. Обобщенная схема взаимодействия администратора ИБ ЕИТС и оператора

ЕИТС по обработке инцидентов ИБ, где:

А) – администратор ИБ ЕИТС,

О) – оператор ЕИТС,

У) – уполномоченный орган.

3.2. Выявление инцидента ИБ

3.2.1. Выявление инцидента ИБ производится исходя из информации, полученной из следующих источников событий безопасности:

- журналы событий, включенных в процесс мониторинга узлов безопасности;
- системы обнаружения вторжений, установленных в ЕИТС;
- антивирусные средства защиты информации;
- журналы средств защиты информации от несанкционированного доступа;
- средства анализа уязвимостей;
- система обнаружения вторжений СОПКА;
- иные, включая деятельность оператора ЕИТС и обращения пользователей ЕИТС.

3.2.2. Выявление инцидентов ИБ выполняется в пределах ЕИТС силами администратора ИБ ЕИТС.

3.2.3. В случае обнаружения инцидента ИБ на компоненте ЕИТС, не являющимся узлом безопасности, приоритет по устранению данного инцидента ИБ устанавливается не выше «средний».

3.2.4. В случае необходимости присвоения инциденту ИБ приоритета «высокий» и «очень высокий» в отношении компонента ЕИТС, не отнесенного к узлу безопасности, администратор ИБ ЕИТС направляет запрос оператору ЕИТС на заполнение и передачу анкеты узла безопасности на данный компонент ЕИТС. Ответ на указанный запрос оператор ЕИТС предоставляет в срок, не превышающий времени реакции на инцидент ИБ.

3.2.5. В случае обнаружения признаков инцидента ИБ оператором ЕИТС, указанные признаки передаются администратору ИБ ЕИТС с целью проведения их исследования на предмет соответствия инциденту ИБ.

Выявление инцидента ИБ производится администратором ИБ ЕИТС 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 инцидентов ИБ.

3.2.6. Для применения нестандартных правил выявления инцидентов ИБ в отношении определенного узла оператор ЕИТС совместно с администратором ИБ ЕИТС формирует специфический для определённого узла (группы узлов ИБ) набор требований к очередности и качеству событий безопасности, поступающих от источников событий безопасности, которые необходимо считать инцидентом ИБ для данного узла безопасности, с указанием причин отнесения данной информации к инциденту ИБ.

3.2.7. По факту получения требований для формирования нестандартных правил выявления инцидентов ИБ администратор ИБ ЕИТС 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 администратор ИБ ЕИТС уведомляет оператора ЕИТС.

3.2.8. В случае невозможности или затруднения реализации указанных нестандартных правил выявления инцидентов ИБ, администратор ИБ ЕИТС в срок, не превышающий 7 рабочих дней, уведомляет оператора ЕИТС и(или) уполномоченный орган с указанием объективных причин.

3.2.9. По факту выявления инцидента ИБ на узле безопасности, включенного в процесс мониторинга, администратор ИБ ЕИТС присваивает регистрационный номер инциденту ИБ, создает карточку инцидента ИБ и вносит в нее параметры событий безопасности, которые первично относят их к инциденту ИБ.

3.3. Анализ инцидента ИБ

3.3.1. Для подтверждения инцидента ИБ администратор ИБ ЕИТС анализирует события безопасности, которые относятся к данному инциденту ИБ, и сопоставляет их с деятельностью и характеристиками узла безопасности из реестра узлов безопасности и иных доступных источников. По результатам данного анализа администратор ИБ ЕИТС принимает решение о подтверждении инцидента ИБ.

3.3.2. Оценка критичности инцидента ИБ

Для подтвержденного инцидента ИБ администратор ИБ ЕИТС устанавливает приоритет инциденту ИБ исходя из данных реестра узлов безопасности и экспертной оценки.

Приоритет инцидента ИБ – это характеристика инцидента ИБ, определяющая потенциальное (возможное) негативное влияние инцидента ИБ на узел ИБ и ЕИТС в целом, вызванное длительным прерыванием, остановкой функционирования процессов, или нарушением конфиденциальности, целостности и (или) доступности обрабатываемых данных.

Приоритет инцидента ИБ	**Описание потенциального негативного воздействия от инцидента ИБ, показатели времени реакции**
Низкий	Инцидент ИБ не может привести к нарушению работы узла безопасности и(или) снижению производительности процессов узла безопасности, решение инцидента ИБ на текущий момент времени не является критичным. Время реакции на инцидент ИБ – не более 4 часов. Время устранения инцидента ИБ – не более 72 часов.

Средний	Инцидент ИБ может привести к нарушению работы узла безопасности и(или) снижению производительности процессов узла безопасности, но ключевые функции будут выполняться. Время реакции на инцидент ИБ – не более 3 часов. Время устранения инцидента ИБ – не более 48 часов.
Высокий	Инцидент ИБ может привести к нарушению работы узла безопасности и(или) снижению производительности других узлов безопасности и(или) сегментов ЕИТС. Время реакции на инцидент ИБ – не более 1 часа. Время устранения инцидента ИБ – не более 24 часов.
Очень высокий	Инцидент ИБ может привести к приостановке процессов внутри сегментов ЕИТС на длительный срок. Время реакции на инцидент ИБ – не более 1 часа. Время устранения инцидента ИБ – не более 4 часов.

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

3.3.3. Для выявления причин и первоначального источника появления инцидента ИБ администратор ИБ ЕИТС анализирует события безопасности в хронологическом порядке и сопоставляет их с иными событиями безопасности подобного типа. В случае если инцидент ИБ может быть следствием эксплуатации конкретного типа уязвимости, администратор ИБ ЕИТС делает анализ уязвимостей узла на предмет поиска данного конкретного типа уязвимостей.

3.3.4. Для выявления массовости инцидента ИБ (несколько подтвержденных инцидентов ИБ на группу узлов безопасности), а также возможной эскалации инцидента ИБ на иные узлы ЕИТС, администратор ИБ ЕИТС проводит выявление участвующих в инциденте ИБ узлов безопасности. В ходе данных мероприятий администратор ИБ ЕИТС анализирует события безопасности на иных узлах ЕИТС на предмет совпадения по признакам выявленного инцидента ИБ. Также в случае, если выявленный инцидент ИБ

имеет отношение с возможным получением прав доступа на узле безопасности, администратор ИБ ЕИТС проводит работы по выявлению подозрительной активности на этом узле безопасности и анализирует состояние узла безопасности на предмет признаков компрометации.

3.3.5. В случае если каких-либо сведений недостаточно для выполнения работ согласно п.3.3.1. – 3.3.4., администратор ИБ ЕИТС формирует запрос на предоставление информации оператору ЕИТС с указанием конкретных видов информации и предварительным приоритетом инцидента ИБ. Оператор ЕИТС предоставляет администратору ИБ ЕИТС указанную информации в срок, не превышающий время реакции на инцидент ИБ.

3.3.6. В случае не подтверждения инцидента ИБ, по которому проводился анализ, администратором ИБ ЕИТС он переводится в статус «закрытый». В карточку инцидента ИБ вносится информации, являющаяся ключевой в ходе не подтверждения инцидента ИБ. Администратор ИБ ЕИТС корректирует правила выявления инцидента ИБ с целью недопущения подобных ложных срабатываний.

3.3.7. По результатам выполнения п. 3.3.1. – 3.3.4 временного регламента и при необходимости выполнения п.3.3.5. администратор ИБ ЕИТС формирует алгоритм устранения инцидента ИБ, в котором описывает очередность действий с целью прекращения влияния инцидента ИБ, недопущения его распространения на другие узлы безопасности и компоненты ЕИТС, блокирования (локализации) источника инцидента ИБ, устранение причин возникновения и устранение его последствий. Алгоритм устранения инцидента ИБ должен содержать набор конкретных операций для ответственного за устранение инцидента ИБ, разбитый по этапам.

3.3.8. Администратор ИБ ЕИТС исходя из полномочий, переданных уполномоченным органом на выполнение государственных работ, определяет может ли устранить инцидент ИБ самостоятельно или же для устранения

потребуется привлечение оператора ЕИТС. В случае если может устранить самостоятельно, тогда администратор ИБ ЕИТС является ответственным исполнителем за устранение инцидента ИБ. В иных случаях, ответственными исполнителями за устранение инцидента ИБ являются оператор ЕИТС и Администратор ИБ ЕИТС.

3.3.9. Информация по п.3.3.1. – 3.3.5. и п.3.3.6. – 3.3.8. вносится в карточку инцидента ИБ с целью дальнейшего учета. Также формируется связь карточки инцидента ИБ с узлом из реестра узлов безопасности.

3.3.10. Администратор ИБ ЕИТС уведомляет уполномоченный орган о зарегистрированном инциденте ИБ.

3.3.11. В случае, если администратору ИБ ЕИТС требуется привлечение к решению инцидента ИБ оператора ЕИТС, то администратор ИБ ЕИТС направляет информацию по инциденту ИБ по п.3.3.1. – 3.3.5. и 3.3.6. – 3.3.7. оператору ЕИТС в объеме, необходимом для устранения инцидента ИБ.

3.3.12. Оператор ЕИТС с момента получения информации по инциденту ИБ уведомляет администратора ИБ ЕИТС информацией о номере заявки, назначенном сотруднике для устранения инцидента ИБ и контактных данных (электронная почта, номер мобильного телефона) в срок, не превышающий время реакции на инцидент ИБ в соответствии с приоритетом инцидента ИБ.

3.3.13. В случае если оператор ЕИТС также не обладает полномочиями на администрирование узла безопасности или компонента ЕИТС, на которых выявлен инцидент ИБ, оператор ЕИТС уведомляет администратора ИБ ЕИТС и уполномоченный орган о невозможности закрытия указанного инцидента ИБ с указанием объективных причин и ответственного администратора узла безопасности или компонента в срок, не превышающий время реакции на инцидент ИБ в соответствии с приоритетом инцидента ИБ.

3.3.14. В случае получения информации в соответствии с п.3.3.13 настоящего Регламента администратор ИБ ЕИТС от имени должностного лица

уполномоченного органа формирует официальный запрос владельцу (функциональному заказчику) или администратору узла безопасности, на котором выявлен инцидент ИБ с целью установления ответственного за устранение инцидента ИБ, содержащий описание инцидента ИБ и алгоритм его устранения в срок, не превышающий один рабочий день.

3.3.15. В случае выявления критических, с точки зрения администратора ИБ ЕИТС, уязвимостей или параметров, влияющих на безопасность, для устранения указанных уязвимостей и изменения параметров, администратором ИБ ЕИТС устанавливается инциденту ИБ приоритет не ниже «Высокий».

3.4. Устранение инцидента ИБ

3.4.1. Устранение инцидента ИБ происходит в рамках рекомендованного алгоритма, определенного в п.3.3.7., по следующим этапам:

- блокирование источника возникновения инцидента ИБ;
- прекращение зловредного влияния;
- недопущение распространения инцидента ИБ на другие узлы безопасности и компоненты ЕИТС;
- устранение причин возникновения инцидента ИБ;
- устранение последствий инцидента ИБ.

3.4.2. Выполнение отдельных мероприятий по устранению инцидента ИБ могут отличаться от типового алгоритма, представленного в п.3.4.1. в соответствии со спецификой конечного инцидента ИБ.

3.4.3. Устранение инцидента ИБ должно быть произведено в срок, не превышающий время устранения инцидента ИБ в соответствии с его приоритетом. Ответственный за устранение инцидента ИБ распределяет время устранения инцидента ИБ по этапам самостоятельно.

3.4.4. По факту выполнения всех операций, перечисленных в алгоритме устранения инцидента ИБ, ответственный за устранение инцидента ИБ уведомляет уполномоченный орган и, в случае если ответственный за устранение инцидента

ИБ не является администратором ИБ ЕИТС, также уведомляет администратора ИБ ЕИТС с приложением подтверждающих операции материалов.

3.4.5. В случае невозможности устранения инцидента ИБ в установленный срок, ответственный за устранение инцидента ИБ направляет информацию в уполномоченный орган, в копии - администратору ИБ ЕИТС, с указанием объективных причин. Работы по устранению инцидента ИБ продолжаются в период согласования изменения сроков устранения инцидента ИБ.

Уполномоченный орган своим решением согласовывает предложенный срок устранения или определяет иной срок устранения с уведомлением администратора ИБ ЕИТС.

3.4.6. В случае не предоставления информации о закрытии инцидента ИБ или же запроса на увеличение сроков закрытия в установленный срок администратор ИБ ЕИТС уведомляет уполномоченный орган и ответственного за устранение инцидента ИБ каждые 4 часа рабочего времени об отсутствии такой информации.

3.4.7. В случае, если ответственным за устранение инцидента ИБ является организация, не являющаяся оператором ЕИТС или администратором ЕИТС, взаимодействие по устранению данного инцидента ИБ организуются в соответствии с п.3.3.14 настоящего Регламента.

3.5. Контроль устранения инцидента ИБ

3.5.1. По факту получения информации о выполнении всех операций, перечисленных в алгоритме устранения инцидента ИБ, администратор ИБ ЕИТС производит контроль устранения инцидента ИБ, заключающийся в анализе событий безопасности, поступающих от источника, зафиксировавшего инцидент ИБ и других косвенных признаков, на предмет соответствия параметрам инцидента ИБ в срок, не превышающий срок устранения инцидента ИБ в соответствии с его приоритетом.

3.5.2. В случае обнаружения признаков инцидента ИБ администратор ИБ ЕИТС осуществляет дополнительный анализ инцидента ИБ с определением расширенного алгоритма устранения инцидента ИБ с возможным определением нового ответственного за устранение инцидента ИБ и его уведомлением в соответствии с имеющимися полномочиями у администратора ИБ, в срок, не превышающий время устранения инцидента ИБ в соответствии с его приоритетом. Администратор ИБ ЕИТС уведомляет уполномоченный орган о продолжении активности, связанной с инцидентом ИБ. Администратор ИБ ЕИТС вносит соответствующую информацию в карточку инцидента ИБ.

3.5.3. Приоритет устранения для инцидента ИБ, который не удалось устранить операциями первоначального алгоритма устранения, устанавливается при отправке ответственному за устранение инцидента ИБ на уровень выше изначального (кроме приоритета «Очень высокий»).

3.5.4. В случае не обнаружения признаков инцидента ИБ в соответствии с п.3.5.1. администратор ИБ ЕИТС уведомляет о подтверждении устранения инцидента ИБ уполномоченный орган и оператора ЕИТС, а также производит процесс закрытия инцидента ИБ.

3.6. Закрытие инцидента ИБ:

3.6.1. По факту подтверждения закрытия инцидента ИБ администратор ИБ ЕИТС в карточке инцидента ИБ переводит его статус в статус «Закрытый», а также вносит информацию о принятых мерах, а также материалы их подтверждающие.

3.6.2. Оператор ЕИТС переводит заявку, связанную с устранением инцидента ИБ в статус «Закрыто».

3.6.3. В случае наличия предпосылок для возникновения подобных закрытому инциденту ИБ иных инцидентов ИБ на узлах ЕИТС администратор ИБ ЕИТС может уведомить уполномоченный орган о возможности реализации оператором ЕИТС алгоритма устранения инцидента ИБ или его части на других

подобных узлах. Сроки выполнения такого рода работ оператор ЕИТС определяет самостоятельно с уведомлением администратора ИБ ЕИТС.

3.6.4. В случае необходимости администратор ИБ ЕИТС вносит корректировки настроек источников событий безопасности и (или) систем анализа событий безопасности с целью оперативного обнаружения инцидентов ИБ подобных закрытому.

Приложение 1

Паспорт
узла безопасности

Производитель оборудования, программного обеспечения	
Тип узла ИБ (нужное подчеркнуть)	Физический сервер/ виртуальная машина /сетевое оборудование / программное обеспечение
Имя узла ИБ	
Наименование и версия системного программного обеспечения	
Краткое описание выполняемых функций	
Способ подключения к узлу ИБ средствами администрирования (нужное подчеркнуть)	SSH, RDP, консольный провод, HTTPS, telnet, SNMP, WMI, RPC, Syslog, WinRM, CIFS/SMB, DCE/RPC, RemoteEngine, LDAP
Способ подключения к узлу ИБ пользователями (нужное подчеркнуть)	Локально, порт-протокол
Адрес расположения (по возможности)	Площадка, наименование организации, CDTO – при наличии
IP-адрес	
Параметры сети устройства (IP-адрес шлюза, VLAN)	
Имеет ли узел ИБ выход в сеть «Интернет»?	Да / Нет
Список ресурсов сети Интернет, необходимых для функционирования компонента ЕИТС (заполняется заблаговременно)	
Влияние на иные процессы в случае выхода из строя/некорректной работы (опционально)	
Наличие технологических связей с другими узлами/ группами узлов (имя узла-тип-технология соединения-IP адрес узла-используемы для соединения порты)	
Перечень административных учетных записей с их правами на данном узле	
Наименование учетной записи с правом администратора для подключения к мониторингу (опционально)	
Для программных серверов	

Перечень прикладного программного обеспечения, установленного на узле и выполняющего основные функции узла (наименование, версия)	
Способ подключения к узлу ИБ для выполнения функций администрирования	SSH, RDP, консольный провод, HTTPS, telnet, SNMP, WMI, RPC, Syslog, WinRM, CIFS/SMB, DCE/RPC, RemoteEngine, LDAP
Перечень вспомогательного программного обеспечения (наименование, версия)	
Специфические особенности (опционально)	

Оператор узла ЕИТС,
Должность, ФИО Дата

Администратор ИБ ЕИТС
Должность, ФИО Дата

Владелец (функциональный заказчик) – по необходимости
Должность, ФИО Дата