ПРАВИТЕЛЬСТВО
АМУРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

28.06.2024 № 512

г. Благовещенск

О создании централизованной
системы управления инцидентами
информационной безопасности

В целях реализации направления (подпрограммы) «Цифровая экономика Амурской области» государственной программы Амурской области «Цифровая трансформация Амурской области», утвержденной постановлением Правительства Амурской области от 22.09.2023 № 792, а также повышения уровня информационной безопасности региональных объектов критической информационной инфраструктуры в сфере здравоохранения Правительство Амурской области

п о с т а н о в л я е т:

1. Государственному бюджетному учреждению Амурской области «Центр информационных технологий Амурской области» (Щербаков С.В.) в срок до 31.10.2024 создать централизованную систему управления инцидентами информационной безопасности (далее – централизованная система).

2. Утвердить Положение о централизованной системе согласно приложению к настоящему постановлению.

3. Министерству здравоохранения Амурской области (Леонтьева С.Н.) совместно с государственным бюджетным учреждением Амурской области «Центр информационных технологий Амурской области» (Щербаков С.В.) обеспечить в срок до 28.12.2024 подключение региональных объектов критической информационной инфраструктуры в сфере здравоохранения к централизованной системе.

4. Контроль за исполнением настоящего постановления возложить на заместителя председателя Правительства Амурской области Пузанова П.И.

5. Настоящее постановление подлежит официальному опубликованию на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru) и размещению на Портале Правительства Амурской области в информационно-телекоммуникационной сети Интернет (www.amurobl.ru).

ПРАВИТЕЛЬСТВО АМУРСКОЙ ОБЛАСТИ
АППАРАТ ГУБЕРНАТОРА ОБЛАСТИ И ПРАВИТЕЛЬСТВА
Отдел регистрации и сопровождения правовых актов

Губернатор Амурской области В.А. Орлов

Приложение
УТВЕРЖДЕНО
постановлением Правительства
Амурской области
от 18.06.2024 № 512

ПОЛОЖЕНИЕ
о централизованной системе управления инцидентами информационной безопасности

1. Общие положения

1.1. Настоящее Положение определяет цели создания, назначение, структуру централизованной системы управления инцидентами информационной безопасности (далее – централизованная система) и функциональные обязанности оператора и участников централизованной системы.

1.2. В настоящем Положении используются следующие основные понятия:

1) централизованная система – комплекс программных и технических средств, направленный на сбор и анализ информации о событиях, связанных с информационной безопасностью в сфере здравоохранения;

2) центр мониторинга и реагирования на инциденты информационной безопасности – организация, осуществляющая лицензируемую деятельность по предоставлению услуг оперативного мониторинга и реагирования на инциденты информационной безопасности, в том числе по взаимодействию с технической инфраструктурой государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

3) инциденты информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий, связанных с информационной безопасностью, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности;

4) региональные объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления участников централизованной системы.

1.3. Оператором централизованной системы является государственное бюджетное учреждение Амурской области «Центр информационных технологий Амурской области».

1.4. Участниками централизованной системы являются владельцы региональных объектов критической информационной инфраструктуры в сфере

здравоохранения (далее – региональные объекты) согласно приложению к настоящему Положению.

2. Цели и назначение централизованной системы

2.1. Централизованная система создана в целях реализации направления (подпрограммы) «Цифровая экономика Амурской области» государственной программы Амурской области «Цифровая трансформация Амурской области», утвержденной постановлением Правительства Амурской области от 22.09.2023 № 792, а также повышения уровня информационной безопасности региональных объектов.

2.2. Централизованная система предназначена для выполнения на региональных объектах следующих функций:

1) сбор, анализ и представление событий, связанных с информационной безопасностью;

2) анализ событий, связанных с информационной безопасностью, в режиме, близком к реальному масштабу времени;

3) хранение и управление данными о событиях, связанных с информационной безопасностью;

4) регистрация и управление инцидентами информационной безопасности;

5) мониторинг событий, связанных с информационной безопасностью;

6) создание отчетов о событиях, связанных с информационной безопасностью.

2.2. Централизованная система обеспечивает единую точку подключения региональных объектов к центру мониторинга и реагирования на инциденты информационной безопасности, а также к системе государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. Структура централизованной системы

3.1. Структура централизованной системы состоит из следующих компонентов:

1) сборщик событий (коллектор), связанных с информационной безопасностью, в функции которого входит:

а) получение данных из источников событий, связанных с информационной безопасностью;

б) приведение необработанного события, связанного с информационной безопасностью, к нормализованному виду в соответствии с заранее заданным для источника и типа события, связанного с информационной безопасностью, правилом нормализации (далее – нормализованное событие);

в) фильтрация нормализованных событий;

г) обогащение и преобразование нормализованных событий;

д) агрегация нормализованных событий;

е) передача нормализованных событий в другие компоненты централизованной системы;

2) коррелятор, в функции которого входит:

а) получение нормализованного события;

б) обнаружение событий, связанных с информационной безопасностью, путем анализа потока нормализованных событий (корреляция);

в) отправка корреляционного события, связанного с информационной безопасностью, в хранилище;

3) хранилище, в функции которого входит хранение нормализованных событий;

4) ядро, в функции которого входит:

а) создание и настраивание сервисов (компонентов) централизованной системы, а также интегрирование в централизованную систему необходимого программного обеспечения;

б) централизованное управление сервисами и учетными записями пользователей – участников централизованной системы;

в) предоставление статистических данных о работе централизованной системы;

г) расследование угроз безопасности на основе полученных событий, связанных с информационной безопасностью.

3.2. Компоненты централизованной системы обеспечивают разделение централизованной системы на сегменты, каждый из которых обрабатывает события, связанные с информационной безопасностью определенного участника централизованной системы, и исключает возможность доступа к ним со стороны других участников централизованной системы.

4. Функциональные обязанности оператора централизованной системы, участников централизованной системы

4.1. Оператор централизованной системы обеспечивает:

1) передачу, установку, настройку, продление неисключительных прав (лицензий) на использование программного обеспечения централизованной системы, а также подключение к ней региональных объектов в рамках финансового обеспечения на соответствующий финансовый год, доведенного до оператора централизованной системы на эти цели;

2) работоспособность программных и технических средств централизованной системы;

3) подключение централизованной системы к сервису центра мониторинга и реагирования на инциденты информационной безопасности в рамках финансового обеспечения на соответствующий финансовый год, доведенного до оператора централизованной системы на эти цели;

4) организацию доступа участников централизованной системы к централизованной системе;

5) осуществление контроля исполнения участниками централизованной системы обязанностей в соответствии с настоящим Положением;

6) анализ статистических показателей централизованной системы;

7) анализ состояния централизованной системы и разработку предложений по развитию централизованной системы.

4.2. Участник централизованной системы обеспечивает:

1) определение лиц, ответственных за мониторинг и реагирование на инциденты информационной безопасности;

2) подключение к централизованной системе следующих устройств, подключенных к сети передачи данных региональных объектов:

а) автоматизированные рабочие места;

б) серверы;

в) виртуальные машины;

г) сетевое оборудование;

3) подключение к централизованной системе следующих источников событий, связанных с информационной безопасностью, региональных объектов:

а) журналы событий, связанных с информационной безопасностью, системного программного обеспечения;

б) средства защиты информации;

в) службы каталогов;

г) базы данных;

д) программное обеспечение сетевого оборудования;

е) средства виртуализации;

ж) почтовые системы;

4) взаимодействие с сервисом центра мониторинга и реагирования на инциденты информационной безопасности;

5) мониторинг событий, связанных с информационной безопасностью, региональных объектов в централизованной системе;

6) реагирование на инциденты информационной безопасности, выявленные централизованной системой;

7) управление инцидентами информационной безопасности, выявленными централизованной системой;

8) анализ отчетов о событиях, связанных с информационной безопасностью, формируемых в централизованной системе.

Приложение
к Положению о централизованной системе управления инцидентами информационной безопасности

Перечень участников централизованной системы управления инцидентами информационной безопасности

№ п/п	Наименование участника централизованной системы управления инцидентами информационной безопасности
1	2
1.	Государственное бюджетное учреждение Амурской области «Центр информационных технологий Амурской области»
2.	Государственное автономное учреждение здравоохранения Амурской области «Амурская областная детская клиническая больница»
3.	Государственное автономное учреждение здравоохранения Амурской области «Амурская областная клиническая больница»
4.	Государственное автономное учреждение здравоохранения Амурской области «Амурская областная инфекционная больница»
5.	Государственное автономное учреждение здравоохранения Амурской области «Амурский областной онкологический диспансер»
6.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурская областная психиатрическая больница»
7.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурский областной кожно-венерологический диспансер»
8.	Государственное автономное учреждение здравоохранения Амурской области «Амурский областной наркологический диспансер»
9.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурский областной противотуберкулезный диспансер»
10.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурский медицинский информационно-аналитический центр»
11.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурский областной детский центр медицинской реабилитации «Надежда»
12.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурское бюро судебно-медицинской экспертизы»
13.	Государственное автономное учреждение здравоохранения Амурской области «Санаторий «Василёк»
14.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурская областная стоматологическая поликлиника»
15.	Государственное бюджетное учреждение здравоохранения Амурской области «Амурская областная станция переливания крови»
16.	Государственное автономное учреждение здравоохранения Амурской области «Амурский областной центр по профилактике и борьбе со СПИД и инфекционными заболеваниями»
17.	Государственное автономное учреждение здравоохранения Амурской области «Белогорская межрайонная больница»
18.	Государственное автономное учреждение здравоохранения Амурской области «Благовещенская городская клиническая больница»
19.	Государственное автономное учреждение здравоохранения Амурской области

1	2
	«Детская городская клиническая больница»
20.	Государственное автономное учреждение здравоохранения Амурской области «Городская поликлиника №1»
21.	Государственное бюджетное учреждение здравоохранения Амурской области «Городская поликлиника № 2»
22.	Государственное автономное учреждение здравоохранения Амурской области «Городская поликлиника № 3»
23.	Государственное автономное учреждение здравоохранения Амурской области «Городская поликлиника № 4»
24.	Государственное автономное учреждение здравоохранения Амурской области «Стоматологическая поликлиника г. Благовещенска»
25.	Государственное бюджетное учреждение здравоохранения Амурской области «Станция скорой медицинской помощи г. Благовещенска»
26.	Государственное бюджетное учреждение здравоохранения Амурской области «Зейская межрайонная больница им. Б.Е. Смирнова»
27.	Государственное бюджетное учреждение здравоохранения Амурской области «Райчихинская городская больница»
28.	Государственное бюджетное учреждение здравоохранения Амурской области «Свободненская межрайонная больница»
29.	Государственное бюджетное учреждение здравоохранения Амурской области «Свободненская городская поликлиника»
30.	Государственное автономное учреждение здравоохранения Амурской области «Тындинская межрайонная больница»
31.	Государственное бюджетное учреждение здравоохранения Амурской области «Тындинская стоматологическая поликлиника»
32.	Государственное бюджетное учреждение здравоохранения Амурской области «Шимановская районная больница»
33.	Государственное автономное учреждение здравоохранения Амурской области «Больница рабочего поселка (пгт) Прогресс»
34.	Государственное бюджетное учреждение здравоохранения Амурской области «Архаринская районная больница»
35.	Государственное бюджетное учреждение здравоохранения Амурской области «Бурейская районная больница»
36.	Государственное бюджетное учреждение здравоохранения Амурской области «Завитинская районная больница»
37.	Государственное автономное учреждение здравоохранения Амурской области «Ивановская районная больница»
38.	Государственное автономное учреждение здравоохранения Амурской области «Константиновская районная больница»
39.	Государственное бюджетное учреждение здравоохранения Амурской области «Магдагачинская районная больница»
40.	Государственное бюджетное учреждение здравоохранения Амурской области «Мазановская районная больница»
41.	Государственное бюджетное учреждение здравоохранения Амурской области «Михайловская районная больница»
42.	Государственное бюджетное учреждение здравоохранения Амурской области «Октябрьская районная больница»
43.	Государственное бюджетное учреждение здравоохранения Амурской области «Ромненская районная больница»

1	2
44.	Государственное бюджетное учреждение здравоохранения Амурской области «Селемджинская районная больница»
45.	Государственное бюджетное учреждение здравоохранения Амурской области «Серышевская районная больница»
46.	Государственное бюджетное учреждение здравоохранения Амурской области «Сковородинская центральная районная больница»
47.	Государственное автономное учреждение здравоохранения Амурской области «Тамбовская районная больница»
48.	Государственное автономное учреждение здравоохранения Амурской области «Больница восстановительного лечения»