



**ПРАВИТЕЛЬСТВО
РЕСПУБЛИКИ МАРИЙ ЭЛ
ПОСТАНОВЛЕНИЕ**

**МАРИЙ ЭЛ РЕСПУБЛИКЫН
ВИКТЕРЖЕ
ПУНЧАЛ**

от 14 мая 2025 г. № 170

г. Йошкар-Ола

**Об утверждении Положения о Центре противодействия
киберугрозам информационным системам
Республики Марий Эл**

В соответствии со статьей 10 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Правительство Республики Марий Эл постановляет:

1. Утвердить прилагаемое Положение о Центре противодействия киберугрозам информационным системам Республики Марий Эл.
2. Контроль за исполнением настоящего постановления возложить на министра цифрового развития Республики Марий Эл.

Председатель Правительства
Республики Марий Эл



Ю.Зайцев

УТВЕРЖДЕНО
постановлением Правительства
Республики Марий Эл
от 14 мая 2025 г. № 170

ПОЛОЖЕНИЕ

о Центре противодействия киберугрозам информационным системам Республики Марий Эл

I. Общие положения

1. Настоящее Положение определяет цели, задачи и порядок деятельности Центра противодействия киберугрозам информационным системам Республики Марий Эл (далее - Центр), созданного на базе государственного бюджетного учреждения Республики Марий Эл «Информсреда» (далее - Учреждение).

2. Целью создания Центра является обнаружение, предупреждение, участие в ликвидации последствий компьютерных атак, реагирование на компьютерные инциденты и взаимодействие с Национальным координационным центром по компьютерным инцидентам (далее - НКЦКИ).

3. При осуществлении своей деятельности Центр руководствуется: Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

приказом Федеральной службы безопасности Российской Федерации от 24 июля 2018 г. № 368 «Об утверждении Порядка 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 Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

приказом Федеральной службы безопасности Российской Федерации от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;

приказом Федеральной службы безопасности Российской Федерации от 19 июня 2019 г. № 282 «Об утверждении Порядка 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»;

приказом Федеральной службы безопасности Российской Федерации от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

нормативными правовыми актами Республики Марий Эл;
методическими документами, разработанными НКЦКИ.

II. Задачи и функции Центра

4. Основными задачами Центра являются:

обнаружение, предупреждение и участие в ликвидации последствий компьютерных атак и реагирование на компьютерные инциденты информационных систем государственных органов Республики Марий Эл (далее - информационные системы Республики Марий Эл), серверов и сервисов телекоммуникационной инфраструктуры государственных органов Республики Марий Эл (далее - информационная инфраструктура Республики Марий Эл);

обеспечение создания общего информационного пространства государственных органов Республики Марий Эл совместно с другими структурными подразделениями Учреждения;

мониторинг, регистрация, предупреждение компьютерных атак и компьютерных инцидентов с помощью средств защиты информации, находящихся в распоряжении Центра;

осуществление анализа угроз информационной безопасности, прогнозирование направления их развития;

сбор и анализ информации о нарушениях информационной безопасности в государственных органах Республики Марий Эл, подготовка предложений по устранению причин их возникновения;

информационно-аналитическое и прогностическое обеспечение функционирования Центра;

иные задачи в соответствии с целями Учреждения по вопросам информационной безопасности.

5. Для реализации поставленных задач Центр осуществляет следующие функции:

установка, настройка и эксплуатация средств обнаружения уязвимостей, предназначенных для обнаружения, предупреждения компьютерных атак и реагирования на компьютерные инциденты информационных систем Республики Марий Эл, серверов и сервисов информационной инфраструктуры Республики Марий Эл;

взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационную инфраструктуру Республики Марий Эл и реагирования на компьютерные инциденты;

представление в НКЦКИ сведений о состоянии защищенности информационной инфраструктуры Республики Марий Эл от компьютерных атак и информации о компьютерных инцидентах в соответствии с установленным порядком;

информирование НКЦКИ об изменении перечня защищаемых информационных ресурсов, предусмотренных пунктом 6 настоящего Положения;

взаимодействие с государственными органами Республики Марий Эл, подведомственными им организациями по вопросам защиты информации;

прием сообщений о событиях информационной безопасности от пользователей информационной инфраструктуры Республики Марий Эл через установленные каналы связи;

составление перечня последствий компьютерных инцидентов в Центре;

установление причин компьютерных инцидентов в Центре;

участие в работах по ликвидации последствий компьютерных атак в Центре;

подготовка отчетов о результатах расследования компьютерных инцидентов;

доведение до системных администраторов государственных информационных систем Республики Марий Эл (далее - ГИС) и информационных систем Республики Марий Эл информации о признаках компьютерного инцидента в целевой информационной системе;

оказание содействия операторам информационных систем Республики Марий Эл в реагировании на инциденты информационной безопасности в целевой информационной системе (при наличии такой необходимости);

разработка документов, регламентирующих процессы обнаружения уязвимостей, обнаружения, предупреждения компьютерных инцидентов и реагирования на компьютерные инциденты в информационной инфраструктуре Республики Марий Эл;

разработка предложений по доработке нормативных правовых актов и методических документов по вопросам кибербезопасности;

предоставление системным администраторам ГИС и информационных систем Республики Марий Эл инструкций по настройке активов в целевой информационной системе для подключения к средствам мониторинга Центра;

проведение работ по периодической проверке информационной инфраструктуры Республики Марий Эл на наличие уязвимостей и организация работ по их устранению;

инвентаризация информационных ресурсов ГИС и информационных систем Республики Марий Эл;

разработка и контроль применения единых методологических требований к процессам создания информационных систем в государственных органах Республики Марий Эл в сфере информационной безопасности совместно с другими структурными подразделениями Учреждения;

организация внедрения технологий формализации описания в электронной форме бизнес-процессов в государственных органах Республики Марий Эл по вопросам информационной безопасности совместно с другими структурными подразделениями Учреждения;

обеспечение выполнения целевых показателей в рамках принятых обязательств между Учреждением и государственными органами Республики Марий Эл, подведомственными им организациями;

консультации в части формирования потребностей по оснащению информационных ресурсов государственных органов Республики Марий Эл средствами комплексной защиты информации совместно с другими структурными подразделениями Учреждения;

составление актов и другой технической документации о степени защищенности технических средств;

контроль за соблюдением нормативных требований по защите информации;

рассмотрение применяемых и предлагаемых методов защиты информации, промежуточных и конечных результатов исследований и разработок;

разработка и реализация мер по устранению выявленных недостатков по защите информации, поиск, обнаружение и организация

устранения уязвимостей в информационных системах Республики Марий Эл;

участие в научных исследованиях, симпозиумах, совещаниях, форумах, в том числе международных, по проблемам защиты информации и информатизации;

иные функции в соответствии с целями и задачами Учреждения.

III. Ответственность Центра

6. Центр несет ответственность за следующие защищаемые информационные ресурсы:

информационные системы государственных органов Республики Марий Эл, подведомственных им организаций, которые размещены на специализированной технологической площадке Учреждения и по которым переданы права на обнаружение, предупреждение и участие в ликвидации последствий компьютерных атак на информационные ресурсы и реагирование на компьютерные инциденты на основании соглашений, договоров, государственных (муниципальных) контрактов;

ГИС, оператором и владельцем которых является Учреждение.

7. Исключение защищаемых информационных ресурсов из пункта 6 настоящего Положения не должно приводить к изменению полноты выполняемых мероприятий по обнаружению, предупреждению и участию в ликвидации последствий компьютерных атак в отношении других информационных ресурсов, за которые Центр несет ответственность.

IV. Права Центра

8. Для достижения поставленных задач Центр вправе:

организовывать обучающие мероприятия по вопросам, входящим в сферу деятельности Центра, и участвовать в них;

участвовать в республиканских, межрегиональных, общероссийских и международных форумах, семинарах, конференциях и иных мероприятиях по вопросам обнаружения, предупреждения, ликвидации последствий компьютерных атак, реагирования на компьютерные инциденты;

запрашивать у государственных органов Республики Марий Эл, подведомственных им организаций информацию и материалы, необходимые для выполнения возложенных на Центр задач и функций.

V. Порядок организации деятельности Центра

9. Центр является структурным подразделением Учреждения. Организационная структура и персональный состав Центра утверждаются приказом Учреждения в соответствии со штатным расписанием Учреждения.

Центр в своей деятельности подчиняется директору Учреждения.

10. Руководство Центром осуществляет главный инженер по защите информации Центра. Главный инженер по защите информации Центра назначается на должность и освобождается от должности директором Учреждения в соответствии с законодательством Российской Федерации по согласованию с Министерством цифрового развития Республики Марий Эл, осуществляющим функции и полномочия учредителя Учреждения.

11. Обязанности главного инженера по защите информации Центра:

1) осуществление оперативного руководства Центром;

2) представление Центра по вопросам, входящим в сферу деятельности Центра, в территориальных органах федеральных органов исполнительной власти в Республике Марий Эл, в том числе осуществляющих контрольно-надзорную деятельность в сфере информационной безопасности, государственных органах Республики Марий Эл, организациях;

3) принятие оперативных мер по противодействию несанкционированному доступу к объектам информатизации и информационным системам, за которые Центр несет ответственность; в случае выявления вероятного или наступившего ущерба от несанкционированного доступа - направление уведомления в устной или письменной форме директору Учреждения и в отдел информационной безопасности Министерства цифрового развития Республики Марий Эл в кратчайшие сроки;

4) иные обязанности, предусмотренные уставом Учреждения, должностной инструкцией.

12. Работники Центра назначаются и освобождаются от должности приказом Учреждения по представлению главного инженера по защите информации Центра. Требования к квалификации и стажу работников Центра, распределение обязанностей между работниками Центра определяются главным инженером по защите информации Центра в соответствии с должностными инструкциями работников Центра и настоящим Положением.

13. Деятельность Центра осуществляется на основе текущего и перспективного планирования, сочетания единоначалия в решении вопросов служебной деятельности и коллегиальности при их обсуждении, персональной ответственности работников

за надлежащее исполнение возложенных на них должностных обязанностей и отдельных поручений руководства Учреждения.

14. Координацию и контроль над деятельностью Центра осуществляет директор Учреждения.

15. Центр создается и ликвидируется на основании решения Правительства Республики Марий Эл.

Реорганизация Центра осуществляется в соответствии с приказом Учреждения по согласованию с Министерством цифрового развития Республики Марий Эл.
