Об утверждении Регламента обеспечения кибербезопасности платформы "цифрового правительства"

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 7 августа 2026 года № 462/НҚ

В соответствии с подпунктом 6) пункта 1 статьи 7-4 Закона Республики Казахстан " О кибербезопасности" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Регламент обеспечения кибербезопасности платформы " цифрового правительства".

2. Комитету по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

1) размещение настоящего приказа на интернет-ресурсе Министерства искусственного интеллекта и цифрового развития Республики Казахстан после его официального опубликования;

2) направление копии настоящего приказа в Республиканское государственное предприятие на праве хозяйственного ведения "Институт законодательства и правовой информации Республики Казахстан" Министерства юстиции Республики Казахстан в течении пяти календарных дней со дня подписания приказа для включения в эталонный контрольный банк нормативных правовых актов Республики Казахстан.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра искусственного интеллекта и цифрового развития Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Заместитель Премьер - Министра –
Министр искусственного интеллекта и цифрового развития Республики Казахстан *Ж. Мадиев*

"СОГЛАСОВАНО"
Комитет национальной безопасности
Республики Казахстан

Утверждены приказом
Заместителя – Премьер -
Министра – Министр
искусственного интеллекта
и цифрового развития
Республики Казахстан
от 7 августа 2026 года № 462/НҚ

Регламент обеспечения кибербезопасности платформы "цифрового правительства"

Глава 1. Общие положения

1. Настоящий Регламент обеспечения кибербезопасности платформы "цифрового правительства" (далее – Регламент) разработан в соответствии с подпунктом 6) пункта 1 статьи 7-4 Закона Республики Казахстан "О кибербезопасности" и определяет последовательность, сроки выполнения работ, порядок оформления результатов работы при осуществлении акционерным обществом "Государственная техническая служба" (далее – АО "ГТС") совместно с акционерным обществом "Национальные информационные технологии" (далее – АО "НИТ") мероприятий по обеспечению кибербезопасности платформы "цифрового правительства" и цифровых объектов размещенных на ней, а также минимальные квалификационные требования к сотрудникам, участвующим в обеспечении кибербезопасности, и описывает процедуры их обучения и повышения квалификации.

2. В настоящем Регламенте используются следующие термины, определения и сокращения:

1) СКЗИ – средство криптографической защиты информации;

2) СУКБ – система управления кибербезопасности (SIEM);

3) СЗИ – средство защиты информации;

4) АИК – анализ исходных кодов;

5) ПО – программное обеспечение;

6) БРПО – безопасная разработка ПО;

7) СВ – среда виртуализации;

8) СУБД – система управления базами данных;

9) Недекларированные возможности (далее – НДВ) – функциональные возможности ПО, не отраженные или не соответствующие описанным в технической документации;

10) ЕШДИ – единый шлюз доступа к Интернету;

11) КБ – кибербезопасность;

12) ТД КБ – техническая документация по кибербезопасности;

13) ППО – прикладное программное обеспечение;

14) ППРК ЕТ – Единые требования в сферах цифровизации и обеспечения кибербезопасности, утверждаемые Правительством Республики Казахстан в соответствии с Законом Республики Казахстан "О кибербезопасности";

15) НПА – нормативные правовые акты Республики Казахстан;

16) ОС – операционная система;

17) ТЗ – техническое задание;

18) уполномоченный орган – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере обеспечения кибербезопасности;

19) фреймворки – совокупность программных библиотек и инфраструктурных компонентов, задающих структуру ПО и обеспечивающих типовые механизмы разработки (маршрутизацию, обработку запросов, доступ к данным);

20) ЦО – цифровой объект;

21) собственник ЦО – субъект, обладающий правом по своему усмотрению владеть, пользоваться и распоряжаться принадлежащим ему ЦО;

22) ЦО ЦП – цифровые объекты "цифрового правительства";

23) платформа "цифрового правительства" (далее – Платформа QazTech) – цифровая платформа оператора "цифрового правительства", предназначенная для разработки, развития, размещения, интеграции цифровых объектов;

24) СЭД – система электронного документооборота;

25) Anti-DDoS – защита цифрового объекта от действий злоумышленников, направленных на нарушение его работоспособности;

26) AV – система обнаружения и предотвращения вредоносных программ;

27) Container security – анализ безопасности собранных Docker-образов;

28) DAST – динамический анализ безопасности приложений (Dynamic Application Security Testing);

29) DLP – СЗИ, предназначенное для предотвращения утечек цифровых ресурсов ограниченного доступа;

30) EDR – система обнаружения и реагирования на сложные угрозы на конечных точках (Endpoint Detection and Response);

31) Gitlab – система хранения и управления репозиториями исходного кода;

32) IaC security – анализ безопасности файлов инфраструктуры (Kubernetes, Terraform);

33) IPS/IDS – система обнаружения и предотвращения вторжений;

34) MAST – тестирование безопасности мобильных приложений (Mobile Application Security Testing);

35) NGFW – межсетевой экран нового поколения (Next-Generation Firewall);

36) PAM – система управления доступом пользователей с привилегированными правами (Privileged Access Management);

37) Pentest – метод оценки безопасности цифровых объектов, с использованием техник и инструментов, имитирующих действия злоумышленника, с целью выявления уязвимостей и возможных сценариев атак и предоставление рекомендаций по их устранению и предотвращению;

38) Pipeline CI/CD – конвейер непрерывной интеграции и непрерывного развертывания ПО;

39) Sandbox – изолированная виртуальная среда для анализа поведения подозрительных файлов;

40) SAST – статический анализ безопасности приложений (Static Application Security Testing);

41) SCA – анализ состава программного обеспечения (Software Composition Analysis);

42) SIEM – система мониторинга и управления инцидентами КБ и событиями КБ;

43) Unit-тест – проверка отдельных функций и компонентов системы на корректность работы;

44) WAF – межсетевой экран для защиты веб-приложений (web-application firewall).

Глава 2. Тестирование и анализ качества исходного кода

Процедуры тестирования и анализа качества исходного кода выполняются в конвейере GitLab CI/CD и включают автоматическое модульное тестирование, проверку качества исходного кода и ручное функциональное тестирование.

Автоматическое модульное тестирование (Unit Testing) — проверка отдельных функций и компонентов системы на корректность работы.

Проверка качества исходного кода (Code Quality check) направлена на выявление нарушений стандартов кодирования, потенциальных ошибок и проблем поддержки кода.

Функциональное тестирование является этапом проверки ПО, направленным на подтверждение реализованного функционала соответствию заявленным требованиям и спецификациям.

Основные задачи:

проверка корректности работы реализованных функций и бизнес-логики;

подтверждение соответствия реализованных функций требованиям ТЗ;

проверка качества и читаемости исходного кода;

контроль соблюдения принятых стандартов кодирования и стиля;

выявление ошибок на ранних этапах (через unit-тесты);

управление найденными уязвимостями, включая их классификацию и устранение;

снижение количества ошибок на этапе интеграционного и приемочного тестирования;

повышение стабильности и сопровождаемости ПО.

Автоматическое модульное тестирование (Unit Tests) выполняются на этапе сборки в GitLab CI/CD и служат основой для обеспечения качества кода.

Проверка качества кода проводится автоматически на этапе сборки в Gitlab CI/CD, для этого применяются автоматизированный инструмент.

Функциональные тесты выполняются автоматически после успешного прохождения unit-тестов и проверки качества кода. С обеспечением комплексной проверки поведения системы на уровне пользовательских сценариев.

Тестирование и оценка качества считаются завершенными при успешном прохождении всех проверок, достижении установленных показателей качества, устранении критичных ошибок и согласовании изменений ответственными участниками.

По результатам владельцем объекта формируется отчет, включающий ключевые метрики, выявленные замечания, их статусы и оценку готовности к релизу с рекомендациями по улучшению. Порядок и сроки оформления отчета определяются владельцем объекта.

Работы выполняются АО "НИТ" в части платформы QazTech и владельцами ЦО — в части компонентов.

Глава 3. Процессы безопасной разработки программного обеспечения

Анализ исходных кодов выполняются с помощью встроенных и (или) интегрированных инструментов DevSecOps, которые анализируют исходный код, зависимости, контейнерные образы, инфраструктурные шаблоны и процессы выполнения ПО во время его функционирования.

Выявление уязвимостей в ПО осуществляется в следующем порядке:

1) при запуске pipeline Gitlab автоматически инициирует этапы проверки безопасности;

2) каждый тип анализа выполняется сканером SAST, SCA, DAST, MAST, Container security, IaC security;

3) при обнаружении уязвимостей высокой и средней степени риска выполнение pipeline приостанавливается;

4) исполнитель АО "ГТС" получает отчет для анализа;

5) проводится анализ программных отчетов на наличие ложных срабатываний (ошибочных результатов автоматического анализа, не подтверждающих фактическое наличие уязвимостей);

6) формируется отчет, включающий в себя перечень выявленных уязвимостей ПО с указанием их описания, маршрута (пути к файлу) и степени риска (высокая, средняя, низкая).

7) разработка и реализация плана по устранению выявленных уязвимостей, включая приоритизацию и сроки выполнения.

Выявление НДВ осуществляется в следующем порядке:

1) запуск pipeline Gitlab с автоматическими этапами проверки безопасности;

2) анализ технической документации Платформы QazTech и ЦО, в том числе ТЗ на создание (развитие) цифрового объекта, в части сведений о его назначении, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы;

3) проведение анализа исходного кода Платформы QazTech и ЦО ручным методом:

изучение модульной и логической структуры ПО, а также функциональных модулей и сравнения структур с приведенными в технической документации;

изучение маршрута выполнения функциональных объектов и проверка обрабатывающих данных;

фиксирование НДВ для последующего предоставления в отчете результатов выявления НДВ;

4) В случае выявления недекларированных возможностей специалистами АИК в системе управления проектом создается Issue, в котором фиксируются результаты проведенного анализа, описание выявленной НДВ, а также отчет по результатам анализа и рекомендации по ее устранению.

При отсутствии уязвимостей и НДВ исполнитель выполняет процедуру утверждения в GitLab для дальнейшего продвижения изменений в ветке репозитория.

Настройка инструментов анализа безопасности (SAST, SCA, DAST, MAST, Container security, IaC security), применяемых в процессе безопасной разработки, осуществляется в используемых средствах анализа. Выполняется интеграция средств анализа с системой управления исходным кодом, настройка профилей анализа, уровней критичности, правил обработки результатов, а также настройка прав доступа и журналирования действий пользователей.

Инструменты анализа адаптируются под используемые языки программирования, фреймворки и типы проектов, настраиваются области анализа, исключаются нерелевантные файлы и оптимизируется время выполнения проверок.

Проводится тестирование новых версий и инструментов анализа и подготовка предложений по совершенствованию процессов безопасной разработки ПО.

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" предоставляет исходный код Платформы QazTech, а собственник ЦО предоставляет исходный код ЦО и необходимую документацию к нему.

Глава 4. Мероприятия по обеспечению кибербезопасности Платформы QazTech

1. Разработка Политики кибербезопасности и ТД КБ в соответствии с требованиями ППРК ЕТ.

АО "НИТ" является ответственным за разработку, внесение изменений и дополнений в ТД КБ, при этом АО "ГТС" участвует в согласовании технических документов.

Периодичность: по необходимости, но не реже одного раза в два года.

Форма завершения: утвержденное ТД КБ.

2. Разработка (внесение изменений и дополнений) Методических требований по разработке, развитию, размещению, интеграции ЦО на платформе "цифрового правительства" (далее – Методика). Методика разрабатывается АО "НИТ" совместно с

АО "ГТС" и утверждается уполномоченным органом для дальнейшего обязательного использования собственниками ЦО.

В Методике описываются основные подходы и требования к pipeline CI/CD с использованием инструментов по анализу исходного кода, формам отчетов, этапов согласования изменения в основных ветках кода, правам доступа в проектах и группах. Определяются методы развертывания исходного кода в продуктивную среду с соблюдением требований КБ.

Методика содержит описание бизнес-процессов по загрузке, разработке и развертыванию исходного кода, а также информацию по работе с инструментами Платформы QazTech.

Периодичность: при необходимости.

Форма завершения: Методика.

3. Проведение обследования основного и резервного серверных помещений (центры обработки данных), в которых размещены программное обеспечение и технические средства Платформы QazTech, на соответствие требованиям ППРК ЕТ осуществляется АО "ГТС", при этом АО "НИТ" обеспечивает работникам АО "ГТС", проводящих обследование, беспрепятственный доступ в серверное помещения (центры обработки данных) и к необходимой документации (журналы, договоры и т.п.).

При обследовании серверных помещений (центров обработки данных) работники АО "ГТС" требованиям, отраженных в Параграфе 8 ППРК ЕТ.

Периодичность: 1 раз в год.

Форма завершения: отчет по обследованию.

4. Осуществление обследования серверного оборудования Платформы QazTech на соответствие требованиям КБ (СВ, разделение сред для разработки, тестирования и промышленной эксплуатации, ОС, СУБД, ППО).

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" обеспечивает его работникам доступ к ОС, СУБД, ППО и СВ, а также предоставляют ответственных лиц (администраторов) для демонстрации политик безопасности.

При обследовании серверного оборудования Платформы QazTech работники АО " ГТС" руководствуются требованиям законодательства и стандартов Республики Казахстан в сфере обеспечения КБ.

Периодичность: 1 раз в год.

Форма завершения: отчет по обследованию.

5. Проведение обследования сетевого оборудования Платформы QazTech на соответствие требованиям КБ (конфигурация межсетевых экранов, маршрутизаторов и коммутаторов, разделение сетей).

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" обеспечивает беспрепятственный доступ его работникам и определяет ответственных

сетевых администраторов за демонстрацию и отработку (в случае необходимости) политик безопасности на сетевом оборудовании.

При обследовании сетевого оборудования Платформы QazTech работники АО "ГТС " руководствуются требованиям законодательств и стандартов Республики Казахстан в сфере обеспечения КБ.

Периодичность: 1 раз в год.

Форма завершения: отчет по обследованию.

6. Проведение инструментального сканирования Платформы QazTech для выявления уязвимостей. Сканированию на наличие обновлений, анализ конфигураций, на наличие известных уязвимостей по базе общих уязвимостей и рисков, на соответствие законодательству и стандартам Республики Казахстан в сфере обеспечения КБ, подлежат виртуальные сервера, сетевое оборудование и СВ Платформы QazTech.

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" обеспечивает его работникам удаленный сетевой доступ к серверам и сетевым устройствам с привилегированными правами (типа "root").

Периодичность: 1 раз в полугодие.

Форма завершения: отчет по сканированию.

7. Нагрузочное тестирование Платформы QazTech проводится АО "ГТС" для оценки соблюдения доступности, целостности и конфиденциальности в среде штатной эксплуатации. Нагрузочное тестирование проводится работниками АО "ГТС" с использованием специализированного программного средства на основании автоматических сценариев, в среде штатной эксплуатации, в которой персональные данные заменены на синтетические (фиктивные). Нагрузочное тестирование проводится по количеству точек подключений пользователей и вариантов точек подключения интеграционного взаимодействия. При этом АО "ГТС" определяет сценарий тестирования, временные и количественные характеристики тестирования, согласовывает время проведения тестирования с АО "НИТ".

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" обеспечивает его работников необходимыми доступами к Платформе QazTech для выполнения работ.

Периодичность: 1 раз в полугодие.

Форма завершения: отчет по нагрузочному тестированию.

8. Проведение АИК (SAST, DAST, SCA, НДВ, Container security, IaC security).

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" предоставляет его работникам исходный код Платформы QazTech, и необходимую документацию (журналы, договоры, ТЗ и т.п.).

Периодичность: 1 раз в год.

Форма завершения: отчет по анализу.

9. Обеспечение внутреннего контроля за соблюдением требований ТД КБ, включая обеспечение их исполнения всеми заинтересованными лицами и внешними контрагентами.

Основным исполнителем работ является АО "НИТ".

Периодичность: на постоянной основе.

Форма завершения: утвержденные документы 4-го уровня ТД КБ.

10. Обеспечение внешнего контроля за соблюдением требований ТД КБ.

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" предоставляет его работникам необходимую документацию, обеспечивает доступ к ОС, СУБД, ППО, СВ, СЗИ (SIEM, PAM, AV и другие), а также определяет ответственных лиц (администраторов) для демонстрации политик безопасности.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

11. Управление правами и доступами: подключение всех систем/подсистем и компонентов Платформы QazTech к AD/LDAP.

Основным исполнителем работ является АО "НИТ", а АО "ГТС" участвует в согласовании процессов управления учетными записями (создание, удаление, модификация прав), при этом АО "НИТ" обеспечивает подключение к AD/LDAP всех компонентов (ОС, БД, СВ и другие) Платформы QazTech.

Периодичность: на постоянной основе.

Форма завершения: Заявка в SD.

12. Управление конфигурациями системного и прикладного ПО и эталонных образов.

Основным исполнителем работ является АО "НИТ", а АО "ГТС" участвует в согласовании изменений конфигураций системного и прикладного ПО и эталонных образов, при этом обеспечивается предустановка в них СЗИ.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

13. Резервное копирование и тестирования восстановления резервных копий всех компонентов Платформы QazTech.

Основным исполнителем работ является АО "НИТ", а АО "ГТС" обеспечивает контроль ее исполнения, при этом процедуры резервного копирования и тестирования восстановления резервных копий выполняются в соответствии с требованиями ТД КБ.

Периодичность: согласно срокам установленных в ТД ИБ Платформы.

Форма завершения: журнал резервных копий и тестирования восстановления резервных копий.

14. Безопасность ключей шифрования и паролей (Vault).

АО "НИТ" производит генерацию 4 seal/unseal ключей, необходимых для запуска, перезапуска и восстановления Vault, которые распределяются и передаются по одному

ключу администраторам Платформы QazTech, подразделению КБ АО "НИТ" и два ключа АО "ГТС". Для проведения процедуры запуска, перезапуска и восстановления Vault требуется предоставление минимум трех ключей.

АО "НИТ" производят генерацию и разделения пароля привилегированного пользователя (root token) на три части и предоставляют на одной части пароля администраторам Платформы QazTech, подразделению КБ АО "НИТ" и АО "ГТС".

Создания токенов Vault для собственников ЦО, определение ролей и типов доступа проводится совместно АО "НИТ" и АО "ГТС".

Периодичность: по мере необходимости.

Форма завершения: Первичная генерация seal/unseal закрепляется актом. Остальные процессы фиксируются в журнале событий Vault.

15. Мониторинг работоспособности СЗИ Платформы QazTech.

Основным исполнителем работ является АО "НИТ", при этом АО "ГТС" принимает участие в исполнении контроля состояния источников событий КБ, их параметров и режимов защиты, в том числе оповещения АО "НИТ" о недостатках и ошибках в их функционировании.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

16. Мониторинг и управление цифровой инфраструктурой Платформы QazTech (отслеживание работы серверов и сетевого оборудования, БД, ППО).

АО "НИТ" обеспечивает мониторинг и управление цифровой инфраструктурой Платформы QazTech, в рамках которого осуществляется мониторинг программного обеспечения и технических средств цифровой инфраструктуры Платформы QazTech и обеспечивается журналирование действий ее администраторов и пользователей.

АО "ГТС" осуществляет контроль за реализацией данного требования, проводит ежеквартальный анализ функционирования систем мониторинга и управления цифровой инфраструктурой Платформы QazTech, предоставляет рекомендации по устранению выявленных несоответствий.

Периодичность: на постоянной основе, ежеквартальный анализ функционирования систем.

Форма завершения: исполнение.

17. Установка и конфигурирование СУКБ и СЗИ классов AV, EDR, Sandbox, DLP.

Процессы по установке и конфигурированию СУКБ и СЗИ осуществляются АО " НИТ", при этом АО "ГТС" принимает участие и оказывает консультационную поддержку по установке программных средств СУКБ (SIEM) и источников событий КБ (AV, EDR, Sandbox, DLP), а также по настройке отдельных механизмов функционирования и политик безопасности источников событий КБ.

Периодичность: по мере необходимости.

Форма завершения: акт установки.

18. Установка и конфигурирование СЗИ классов IDS/IPS/NGFW.

АО "НИТ" осуществляет, а АО "ГТС" участвует в установке и конфигурации технических средств IDS/IPS/NGFW: монтаж, настройка СЗИ классов IDS/IPS/NGFW.

Периодичность: по мере необходимости.

Форма завершения: акт установки.

19. Установка и конфигурирование СЗИ классов PAM.

АО "НИТ" (при необходимости – совместно с АО "ГТС") осуществляет развертывание и настройку системы PAM для контроля действий администраторов Платформы QazTech и администраторов осуществляющих сопровождение серверов ЦО в продуктивной среде Платформы QazTech.

АО "ГТС" определяет требования по настройке политик системы PAM, ролей, прав доступа и отправки журналов в SIEM систему.

АО "НИТ" регистрирует и учет пользователей в PAM-системе, обеспечивает соблюдение требований АО "ГТС".

Периодичность: по мере необходимости.

Форма завершения: акт установки.

20. Подключение источников событий к Платформе QazTech.

Подключение источников событий к СУКБ (SIEM) Платформы QazTech.

Процессы по подключению источников событий к цифровой инфраструктуре Платформы QazTech осуществляются АО "НИТ", при этом АО "ГТС" принимает участие и оказывает консультационную поддержку по настройке отдельных механизмов функционирования и политик безопасности СУКБ (SIEM), проверку корректности работы, а также по обеспечению централизованного сбора сведений из журналов регистрации событий в СУКБ (SIEM).

Периодичность: по мере необходимости.

Форма завершения: исполнение.

21. Контроль состояния источников событий КБ, их параметров и режимов защиты, в том числе устранение ошибок и недостатков в их функционировании

Контроль состояния источников событий КБ, их параметров и режимов защиты, в том числе устранение ошибок и недостатков в их функционировании осуществляется АО "НИТ", при этом АО "ГТС" принимает участие и оказывает консультационную поддержку при обращении АО "НИТ" по контролю работоспособности серверного оборудования, ОС, ПО СЗИ и доступности каналов связи между Платформой QazTech и источниками событий КБ.

Периодичность: по мере необходимости.

Форма завершения: исполнение.

22. Настройка политики (правил) СЗИ классов AV, EDR, Sandbox.

АО "НИТ" осуществляет периодическое изменение параметров конфигурации (политики) СЗИ классов AV, EDR и Sandbox для Платформы QazTech в соответствии с

технической документацией и рекомендациями производителя СЗИ. АО "ГТС" осуществляет диагностику корректного функционирования СЗИ на основе журналов событий, и, при необходимости, уведомляет АО "НИТ" о недостатках в параметрах конфигурации (политиках).

Изменение параметров конфигурации (политик), диагностика и устранение недостатков в них может осуществляться по заявкам (запросу) АО "НИТ".

Периодичность: при необходимости.

Форма завершения: измененные политики.

23. Настройка политик (правил) СЗИ классов IDS/IPS/NGFW и PAM, DLP в части КБ.

АО "ГТС" определяет требования по настройке политик системы PAM, ролей, прав доступа.

АО "НИТ" обеспечивает настройку политик и соблюдение требований АО "ГТС".

Периодичность: при необходимости.

Форма завершения: исполнение.

24. Обеспечение пропуска интернет-трафика Платформы QazTech через ЕШДИ на всех этапах жизненного цикла.

АО "НИТ" обеспечивает, а АО "ГТС" принимает участие в подключении интернет-трафика через ЕШДИ, настройке политик доступа в соответствии с ППРК ЕТ, а также проводит мониторинг и анализ трафика на предмет наличия аномалий, вредоносного ПО.

АО "НИТ" обеспечивает канал связи и подключает Платформу QazTech к ЕШДИ.

Периодичность: при необходимости.

Форма завершения: исполнение.

25. Анализ поступающих в СУКБ данных с целью создания правил корреляции и алгоритмов выявления угроз и инцидентов КБ.

Основным исполнителем работ является АО "ГТС". При проведении работ понаписанию правил корреляции и алгоритмов выявления угроз и инцидентов КБ, АО "НИТ" обеспечивает для его работников удаленный сетевой доступ к СУКБ с привилегированными правами (учетная запись с правами "root") .

В случае выявления посредством СЗИ класса AV, EDR и Sandbox на Платформе QazTech целевых кибератак, АО "ГТС" создает соответствующие правила корреляции, учитывающие релевантные тактики, техники и процедуры, артефакты конечных точек, сетевые артефакты и индикаторы компрометации.

Периодичность: ежедневно.

Форма завершения: правила на СУКБ.

26. Мониторинг событий на СУКБ и СЗИ на наличие следов злоумышленника (1-й уровень).

Основным исполнителем работ является АО "НИТ".

АО "НИТ" проводит круглосуточный мониторинг и первичное реагирование на инциденты КБ посредством СУКБ и СЗИ Платформы QazTech с целью обнаружения инцидентов КБ.

Периодичность: круглосуточно.

Форма завершения: круглосуточный мониторинг, исполнение.

27. Фильтрация сетевого трафика на ЕШДИ (WAF, Anti-DDoS, IPS).

АО "ГТС" обеспечивает, при этом АО "НИТ" (в случае необходимости) участвует в настройке политик доступа, настройке сигнатур и необходимых СЗИ на оборудованиях ЕШДИ.

Периодичность: по необходимости.

Форма завершения: исполнение.

28. Тестирование на проникновение (Pentest/Red Team) в "ручном" режиме.

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" обеспечивает его работникам удаленный сетевой доступ к серверам и сетевым устройствам с ограниченными правами (типа "user").

АО "ГТС" проводит Pentest Платформы QazTech на наличие уязвимостей в режиме "ручного" тестирования.

Периодичность: 1 раз в полугодие.

Форма завершения: заключение по результатам проведения Pentest.

29. Инструментальное сканирование Платформы QazTech для выявления уязвимостей.

Проведение инструментального сканирования для выявления уязвимостей. Сканирование на наличие обновлений и анализ конфигурации, на наличие известных уязвимостей ПО по базе общих уязвимостей и рисков, на соответствие законодательству и стандартам Республики Казахстан в сфере обеспечения КБ, подлежат СВ, сетевое оборудование и виртуальные серверы Платформы QazTech.

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" обеспечивает его работникам удаленный сетевой доступ к серверам и сетевым устройствам с привилегированными правами (учетная запись с правами "root").

Периодичность: 1 раз в полугодие.

Форма завершения: отчет по сканированию.

30. Мониторинг КБ и первичное реагирование на инциденты КБ (1-я линия).

Основным исполнителем работ является АО "НИТ".

АО "НИТ" проводит круглосуточный мониторинг и первичное реагирование на инциденты КБ посредством СУКБ Платформы QazTech с целью обнаружения инцидентов КБ.

Периодичность: круглосуточно.

Форма завершения: круглосуточный мониторинг, исполнение.

31. Реагирование на инциденты КБ (2-я линия).

В рамках второй линии реагирования АО "ГТС" оказывает содействие заявителям в расследовании инцидентов КБ, анализе артефактов, сборе дополнительной информации и подготовке рекомендаций по устранению угроз/инцидентов КБ. При необходимости инциденты КБ эскалируются на третью/четвертую линию реагирования
.

Периодичность: по необходимости (оказание содействия по отработке инцидентов КБ осуществляется АО "ГТС" совместно с АО "НИТ" в течение рабочего дня, либо по графику пассивного дежурства 2 линии в выходные/праздничные дни при критичных инцидентах).

Форма завершения: предоставление отчета/рекомендаций в адрес АО "НИТ" или эскалация на третью/четвертую линию реагирования.

32. Реагирование на инциденты КБ (3-я линия).

АО "ГТС" обеспечивает поддержку на третьей линии реагирования, которая включает техническую и экспертную поддержку расследования – проведение анализа причин возникновения инцидента КБ, форензики, исследования артефактов, выработки мер по предотвращению повторения инцидента КБ и передачи в АО "НИТ" отчета по результатам анализа.

Периодичность: по факту поступления инцидентов КБ от второй линии реагирования (в течение рабочего дня, либо по графику пассивного дежурства 3 линии в выходные/праздничные дни при критичных инцидентах КБ).

Форма завершения: исполнение, подготовка отчета или передача на четвертую линию реагирования.

33. Реагирование на инциденты КБ (4-я линия).

АО "ГТС" для реагирования на целевые кибератаки, при необходимости, производит следующие мероприятия:

первичное исследование инструментов и утилит посредством базового статического и динамического анализа;

исследование дампов оперативной памяти, выявление и извлечение подозрительных процессов и артефактов;

исследование дампов жестких дисков серверов.

АО "НИТ" обеспечивает получение объектов исследования. По результатам проведенного исследования составляется отчет по форме, определенной во внутренних актах АО "ГТС".

Форма завершения: отчет по результатам исследования.

34. Исправление уязвимостей и недостатков, выявленных по результатам реагирования на инциденты КБ.

АО "НИТ" принимает соответствующие меры по исправлению уязвимостей и недостатков, выявленных по результатам реагирования на инциденты, при этом АО " ГТС" осуществляет контроль проведенных работ.

АО "НИТ" в рамках исправления уязвимостей и недостатков может запросить у АО "ГТС" подробную информацию с рекомендациями о последовательности действий по устранению новой уязвимости, ранее не встречающейся в практике.

Периодичность: по мере выявления уязвимости.

Форма завершения: исполнение.

35. Информирование собственников ЦО о выявленных инцидентах КБ в рамках реактивного сервиса (реагирование на инциденты КБ).

Основным исполнителем работ является АО "НИТ". АО "НИТ" предпринимает соответствующие меры совместно с собственником ЦО.

Периодичность: на постоянной основе, по мере обнаружения инцидентов КБ.

Форма завершения: уведомление.

Глава 5. Мероприятия по обеспечению КБ ЦО (разработка)

36. Разработка ЦО в соответствии с методологии безопасной разработки. Собственники ЦО соблюдают требования настоящей методические рекомендации. Также АО "НИТ" предоставляют все необходимые вычислительные ресурсы и инструменты собственникам ЦО.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

37. Разработка модели угроз КБ для ЦО

Основным исполнителем работ является собственник ЦО, который утверждает модель угроз КБ, а АО "ГТС" согласовывает документ.

Периодичность: по необходимости.

Форма завершения: документ.

38. Согласование ТЗ на ЦО

Основным исполнителем данной работы является уполномоченный орган, согласно подпункту 23) статьи 7-1 Закона. При этом АО "ГТС", в соответствии с подпунктом 3) пункта1 статьи 14 Закона, проводит экспертизу ТЗ на создание или развитие ЦО " цифрового правительства" на соответствие требованиям КБ.

Периодичность: на постоянной основе.

Форма завершения: ТЗ, согласованное с уполномоченным органом.

39. Организация доступа собственникам ЦО к АИК на Портале QazTech.

Основным исполнителем работ является АО "НИТ", при этом АО "ГТС" осуществляет согласование указанных доступов.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

40. Проведение Unit-теста (проверки функционала) и проверка качества кода осуществляется собственниками ЦО с целью разработки ЦО строго в соответствии с ТЗ

.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

41. Проведение АИК (SAST, DAST, MAST, SCA, Container security, IaC security) в среде разработки осуществляется собственниками ЦО при использовании инструментов (анализаторов), реализованных на Платформе QazTech.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

42. Анализ исходного кода (SAST, DAST, MAST, SCA, Container security, IaC security, Unit-тест). Собственникам ЦО предоставляется возможность самостоятельно провести процедуры анализа исходного на этапе тестирования перед размещением ЦО в среде эксплуатации.

Периодичность: на постоянной основе.

Форма завершения: анализ исходного кода.

43. Заявка на размещение в PROD (при наличии согласованного ТЗ). Собственники ЦО перед размещением его в среде PROD (среда эксплуатации) подают соответствующую заявку в АО "НИТ", при этом АО "НИТ" принимает заявку в работу, а АО "ГТС" согласовывает либо отклоняет заявку.

Периодичность: на постоянной основе.

Форма завершения: размещение либо мотивированный отказ в размещении ЦО в PROD.

44. Инструментальное сканирование для выявления уязвимостей.

Проведение инструментального сканирования (в среде PROD) для выявления уязвимостей. Сканирование на наличие обновлений и анализ конфигурации, на наличие известных уязвимостей ПО осуществляется по базе общих уязвимостей и рисков, на соответствие стандартам в сфере обеспечения КБ. Сканированию подлежат виртуальные сервера.

Основным исполнителем работ является АО "ГТС", при этом собственники ЦО и (или) АО "НИТ" обеспечивают его работникам удаленный сетевой доступ к серверам и сетевым устройствам с привилегированными правами (типа "root").

Периодичность: 1 раз в год.

Форма завершения: отчет по сканированию.

45. Проверка ЦО на соответствие требованиям законодательства и стандартов Республики Казахстан в сфере обеспечения КБ.

Основным исполнителем работ является АО "ГТС", при этом собственники ЦО обеспечивают предоставление соответствующих доступов для выполнения указанных работ.

Периодичность: при каждом изменении.

Форма завершения: отчет по проверке.

46. Политика кибербезопасности и ТД КБ на ЦО.

Собственники ЦО при участии АО "НИТ" разрабатывают ТД КБ в виде четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов, которыми руководствуются пользователи. АО " ГТС" обеспечивает контроль при разработке документации.

Периодичность: при внедрении ЦО и с дальнейшим пересмотром в соответствии с ППРК ЕТ.

Форма завершения: утвержденная собственником ЦО ТД КБ.

47 Разработка конфигурации для Pipeline CI/CD в части разработки и размещения ЦО на Платформе QazTech.

Собственник ЦО производит разработку Pipeline CI/CD в рамках разрабатываемого ЦО согласно методической рекомендации.

АО "ГТС" изучает содержимое и конфигурацию Pipeline CI/CD собственника ЦО, проводит анализ на соответствие документации, после чего согласовывает Pipeline CI/CD для дальнейшего использования в проекте на Платформе QazTech. Изменения Pipeline CI/CD, который используется для развертывания кода в продуктивной среде проходят процедуру согласования с АО "ГТС".

Периодичность: на постоянной основе.

Форма завершения: конфигурация для Pipeline CI/CD в части разработки и размещения ЦО на Платформе QazTech.

48. Разработка конфигурации для Pipeline CI/CD в части обеспечения КБ

Собственник ЦО производит разработку Pipeline CI/CD в рамках разрабатываемого ЦО согласно Методики безопасной разработки по настройки конфигурации для Pipeline CI/CD в части обеспечения КБ.

АО "ГТС" проводит анализ Pipeline CI/CD собственника ЦО и согласовывает формат и содержание Pipeline CI/CD для дальнейшего использования в проекте на Платформе QazTech.

Периодичность: на постоянной основе.

Форма завершения: конфигурация для Pipeline CI/CD в части обеспечения КБ.

49. Согласование на интеграцию с другими ЦО ЦП.

При необходимости обеспечения взаимодействия ЦО с другими ЦО ЦП, собственники ЦО направляют заявку на интеграцию, АО "НИТ" обеспечивают интеграцию по согласованию с АО "ГТС".

Периодичность: на постоянной основе.

Форма завершения: согласование или мотивированный отказ.

50. Внутренний контроль за соблюдением требований ТД КБ на ЦО.

АО "НИТ" обеспечивает внутренний контроль за соблюдением требований ТД КБ на ЦО, при этом собственник ЦО обеспечивает участие своего ответственного лица при выполнении работ по контролю.

Периодичность: 1 раз в год.

Форма завершения: отчет.

51. Внешний контроль за соблюдением требований ТД КБ в ЦО.

АО "ГТС" обеспечивает внешний контроль за соблюдением требований ТД КБ в ЦО, при этом АО "НИТ" и собственники ЦО обеспечивают участие своих ответственных лиц при выполнении работ.

Периодичность: 1 раз в год.

Форма завершения: отчет.

52. Проверка ОС, СУБД и ППО на соответствие требованиям КБ, разделение на среды разработки, тестирования и промышленной эксплуатации) - по чек-листу.

АО "ГТС" осуществляет проверку на соответствие требованиям КБ на уровне ОС, СУБД и ППО, при этом АО "НИТ" и собственники ЦО обеспечивают демонстрацию политик безопасности при участии ответственных лиц (администраторов, КБ).

При обследовании серверного оборудования Платформы QazTech работники АО " ГТС" руководствуются требованиями законодательства и стандартов Республики Казахстан в сфере обеспечения КБ.

Периодичность: 1 раз в год.

Форма завершения: отчет.

53. Проверка на соответствие требованиям законодательства и стандартов Республики Казахстан в сфере обеспечения КБ.

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" и собственники ЦО предоставляет необходимые доступы для проведения указанных работ.

Периодичность: 1 в год.

Форма завершения: отчет.

54. Проведение инструментального сканирования для выявления уязвимостей.

Сканирование на наличие обновлений и анализ конфигурации, на наличие известных уязвимостей ПО из базы общих уязвимостей и рисков, на соответствие стандартам в сфере обеспечения КБ, подлежат виртуальные сервера, сетевое оборудование в рамках ЦО.

Основной исполнитель по видам работ является АО "ГТС", при этом АО "НИТ" и собственники ЦО обеспечивает его работникам удаленный сетевой доступ к серверам и сетевым устройствам с привилегированными правами (типа "root").

Периодичность: 1 раз в полугодие.

Форма завершения: отчет по сканированию.

55. Нагрузочное тестирование.

Нагрузочное тестирование ЦО проводится для оценки соблюдения доступности, целостности и конфиденциальности в среде штатной эксплуатации. Нагрузочное тестирование проводится с использованием специализированного программного средства на основании автоматических сценариев, в среде штатной эксплуатации, в

которой персональные данные заменены на фиктивные. Нагрузочное тестирование проводится по количеству точек подключений пользователей и вариантов точек подключения интеграционного взаимодействия. При этом, определяется сценарий тестирования, временные и количественные характеристик тестирования, согласовывается время проведения тестирования с собственниками ЦО.

Основным исполнителем работ является АО "ГТС", при этом собственники ЦО обеспечивает его работников необходимыми доступами для выполнения работ.

Периодичность: 1 раз в полугодие или при каждом изменении.

Форма завершения: отчет по нагрузочному тестированию.

56. Тестирование на проникновение (Pentest/Red Team) в "ручном" режиме.

Основным исполнителем работ является АО "ГТС", при этом АО "НИТ" и собственники ЦО обеспечивает удаленный сетевой доступ к серверам и сетевым устройствам с ограниченными правами (типа "user").

АО "ГТС" проводит Pentest в режиме "ручного" тестирования.

Периодичность: 1 раз в полугодие.

Форма завершения: заключение по результатам проведенного Pentest.

57. Настройка конфигурации системного и прикладного ПО и кода Git.

Собственник ЦО совместно с АО "НИТ" производит настройку конфигурации системного и прикладного ПО, а также кода в Git в соответствии с Методикой на Платформе QazTech и требованиям КБ.

АО "ГТС" проводит проверку на соответствие методологии и требованиям КБ и согласовывает применение конфигураций системного и прикладного ПО и кода в Git. АО "ГТС" осуществляет контроль конфигурации системного и прикладного ПО на продуктивных серверах ЦО.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

58. Резервное копирование и тестирования восстановления резервных копий.

АО "НИТ" и собственники ЦО обеспечивают резервное копирование и тестирования восстановления резервных копий ЦО на всех уровнях (ППО, ОС, БД), АО "ГТС" обеспечивает контроль за исполнением.

Периодичность: на постоянной основе в соответствии с ТД КБ.

Форма завершения: исполнение.

59. Безопасность ключей шифрования и паролей (Vault).

Собственник ЦО для обеспечения безопасного хранения и использования чувствительных данных (пароли, токены, ключи шифрования и т.п.) в продуктивной среде используют систему управления секретами (Vault).

АО "НИТ" обеспечивает отправку журналов (в том числе события по использованию ключей) системы Vault в SIEM. АО "ГТС" осуществляет контроль по отправке журналов и мониторинг событий по использованию ключей.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

60. Установка и конфигурирование СЗИ классов AV, EDR, Sandbox.

Процессы по установке и конфигурированию СЗИ осуществляются АО "НИТ", при этом АО "ГТС" осуществляет контроль проведенных работ по установке программных средств источников событий КБ (AV, EDR, Sandbox), а также по настройке отдельных механизмов функционирования и политик безопасности источников событий КБ.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

61. Установка и конфигурирование СЗИ классов IDS/IPS/NGFW виртуал. и PAM.

АО "ГТС" согласовывает настройки политик системы PAM, ролей, прав доступа и контролирует их применение. АО "НИТ" производит установку и конфигурирование системы контроля привилегированных пользователей Платформы QazTech, а также обеспечивает настройку политик.

АО "НИТ" производит монтаж и конфигурирование СЗИ классов IDS/IPS/NGFW, при этом АО "ГТС" осуществляет контроль установки и настройки СЗИ классов IDS/IPS/NGFW.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

62. Подключение источников событий к Платформе QazTech.

Процессы по подключению источников событий к цифровой инфраструктуре Платформы QazTech осуществляются собственником ЦО и АО "НИТ", при этом АО " ГТС" осуществляет согласование и контроль проведенных работ по настройке отдельных механизмов функционирования и политик безопасности СУКБ (SIEM), проверку корректности работы, а также по обеспечению централизованного сбора сведений из журналов регистрации событий в СУКБ (SIEM).

Периодичность: на постоянной основе.

Форма завершения: исполнение.

63. Контроль состояния источников событий КБ, их параметров и режимов защиты, в том числе устранение ошибок и недостатков в их функционировании.

Контроль состояния источников событий КБ, их параметров и режимов защиты, в том числе устранение ошибок и недостатков в их функционировании осуществляется собственником ЦО и АО "НИТ", при этом АО "ГТС" осуществляет контроль проведенных работ в части работоспособности серверного оборудования, ОС, ПО СЗИ и доступности каналов связи между Платформой QazTech и источниками событий КБ.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

64. Настройка политик СЗИ классов AV, EDR, Sandbox.

АО "НИТ" осуществляет периодическое изменение параметров конфигурации (политики) СЗИ классов AV, EDR и Sandbox для ЦО в соответствии с технической документацией и рекомендациями производителя СЗИ. АО "ГТС" осуществляет диагностику корректного функционирования СЗИ на основе журналов событий, и, при необходимости, уведомляет АО "НИТ" о недостатках в параметрах конфигурации (политиках).

Изменение параметров конфигурации (политик), диагностика и устранение недостатков в их может осуществляться по заявкам (запросу) собственников ЦО.

Периодичность: По мере необходимости.

Форма завершения: измененные политики.

65. Настройка политик СЗИ классов IDS/IPS/NGFW и PAM, DLP.

АО "НИТ" производит установку и конфигурирование системы контроля привилегированных пользователей Платформы QazTech. АО "ГТС" осуществляет согласование и контроль применения политик системы PAM. АО "НИТ" производит настройку политик СЗИ классов IDS/IPS/NGFW, АО "ГТС" обеспечивает контроль применения политик СЗИ классов IDS/IPS/NGFW.

Периодичность: на постоянной основе.

Форма завершения: исполнение.

66. Анализ поступающих в СУКБ данных с целью написания правил корреляции и алгоритмов выявления угроз и инцидентов КБ.

Основным исполнителем работ является АО "НИТ". При проведении работ по написанию правил корреляции и алгоритмов выявления угроз и инцидентов КБ, АО " НИТ" обеспечивает работникам АО "ГТС" удаленный сетевой доступ к СУКБ с привилегированными правами (учетные записи с правами "root").

В случае выявления посредством СЗИ класса AV, EDR и Sandbox на ЦО целевых кибератак, АО "ГТС" создает соответствующие правила корреляции, учитывающие релевантные тактики, техники и процедуры, артефакты конечных точек, сетевые артефакты и индикаторы компрометации.

Периодичность: ежедневно.

Форма завершения: правила на СУКБ.

67. Мониторинг КБ и первичное реагирование на инциденты КБ посредством СУКБ Платформы QazTech (1-я линия).

Основным исполнителем работ является АО "НИТ".

Периодичность: круглосуточно.

Форма завершения: круглосуточный мониторинг, исполнение.

68. Реагирование на инциденты КБ (2-я линия).

В рамках второй линии реагирования АО "ГТС" оказывает содействие заявителям в расследовании инцидентов КБ, анализе артефактов, сборе дополнительной информации и подготовке рекомендаций по устранению угроз/инцидентов КБ. При

необходимости инциденты КБ эскалируются на третью/четвертую линию реагирования
.

Периодичность: по необходимости (оказание содействия по отработке инцидентов КБ осуществляется АО "ГТС" совместно с АО "НИТ" в течение рабочего дня, либо по графику пассивного дежурства 2 линии в выходные/праздничные дни при критичных инцидентах).

Форма завершения: предоставление отчета/рекомендаций в адрес АО "НИТ" или эскалация на третью/четвертую линию реагирования.

69. Реагирование на инциденты КБ (3-я линия).

АО "ГТС" обеспечивает поддержку на третьей линии реагирования, которая включает техническую и экспертную поддержку расследования – проведение анализа причин возникновения инцидента КБ, форензики, исследования артефактов, выработки мер по предотвращению повторения инцидента КБ и передачи в АО "НИТ" отчета по результатам анализа.

Периодичность: по факту поступления инцидентов КБ от второй линии реагирования (в течение рабочего дня, либо по графику пассивного дежурства 3 линии в выходные/праздничные дни при критичных инцидентах КБ).

Форма завершения: исполнение, подготовка отчета или передача на четвертую линию реагирования.

70. Поддержка реагирования на инциденты КБ (4-я линия).

АО "ГТС" для реагирования на целевые кибератаки, при необходимости, производит следующие мероприятия:

первичное исследование инструментов и утилит посредством базового статического и динамического анализа;

исследование дампов оперативной памяти, выявление и извлечение подозрительных процессов и артефактов;

исследование дампов жестких дисков серверов.

АО "НИТ" и собственник ЦО обеспечивают получение указанных объектов исследования. Форма завершения: по результатам проведенного исследования составляется отчет по форме, определенной внутренними актами АО "ГТС".

71. Исправление уязвимостей и недостатков, выявленных по результатам реагирования на инциденты КБ.

Собственник ЦО проводит соответствующие меры по устранению уязвимостей и недостатков, выявленных по результатам реагирования на инциденты КБ, при этом АО "ГТС" осуществляет контроль проведенных работ.

АО "НИТ" в рамках устранения уязвимостей и недостатков может запросить у АО " ГТС" подробную информацию с рекомендациями о последовательности действий по устранению новой уязвимости, ранее не встречающейся в практике.

Периодичность: по мере выявления уязвимости.

Форма завершения: исполнение.

72. Информирование собственников, владельцев и пользователей ЦО ЦП об инцидентах КБ в части их касающейся.

Собственник ЦО информирует заказчика/клиентов о выявленных инцидентах КБ в части их касающейся, при этом АО "ГТС" осуществляет контроль проведенных работ.

Периодичность: по мере выявления инцидента КБ.

Форма завершения: уведомление.