Отчет по мониторингу событий информационной безопасности

Ноябрь, 2025 г.

рег. № 623/1 от 03.12.25 г.

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z120250000
Электронный докумен

Содержание

Оглавление

1. Введение.....3
2. Определения.....4
3. Источники событий.....5
4. Классификация событий ИБ.....6
5. Результаты мониторинга.....7
6. Рекомендации.....10
7. Заключение.....16

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

1. Введение

На основании технической спецификации к договору о государственных закупках услуг №6 от 10.02.2025 г., заключенному между КГУ «Управление цифровых технологий акимата Северо-Казахстанской области» *(далее - Заказчик)* и ТОО «MSSP.GL» *(далее - Исполнитель)*, в ноябре 2025 года, Исполнителем были проведены следующие работы:

1. Мониторинг событий информационной безопасности:

- Круглосуточный мониторинг событий ИБ [1] в режиме 24/7/365 и техническая поддержка;

- Проведение процедур по первичной аналитике и реагированию на инциденты ИБ;

- Обеспечение защищенных каналов взаимодействия между Заказчиком и Поставщиком;

- Мониторинг состояния защищенных каналов передачи журналов событий:

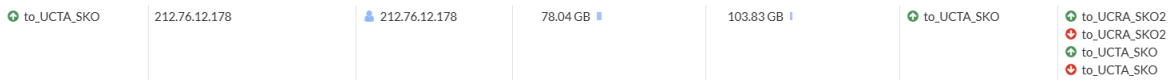

Рисунок 1. Мониторинг туннеля [Заказчик – Исполнитель] для сбора событий ИБ

- Выдача рекомендаций по устранению инцидентов ИБ и дальнейшему их предупреждению.

2. Мониторинг и анализ внешнего цифрового периметра.

- Осуществляется выявление потенциальных уязвимостей, автоматизированный учет активов, проверка ресурсов даркнета и хакерских форумов на предмет выявления утечек данных в пределах корпоративного сегмента, приоритизацию рисков;

- Заказчику предоставлен доступ к личному кабинету системы, для самостоятельной выгрузки, записи и сохранения отчетов сканирования;

- По результатам сканирования сформирован отчет по мониторингу и анализу внешнего цифрового периметра *(приложение 2 к письму)*.

[1] Событие информационной безопасности - состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объекта информатизации

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

2. Определения

В настоящем документе использованы следующие определения:

Информационная безопасность (ИБ) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Оперативный центр информационной безопасности (ОЦИБ) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.

Источник событий ИБ – устройства, генерирующие события (операционные системы, базы данных, прикладное программное обеспечение, средства защиты информации, сетевое и серверное оборудование).

Событие ИБ – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объекта информатизации.

Security Information and Event Management (SIEM) – система мониторинга и управления событиями ИБ.

НКЦИБ – Национальный координационный центр информационной безопасности акционерного общества «Государственная техническая служба».

АО «ГТС» – Акционерное общество «Государственная техническая служба».

Инцидент ИБ – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов.

IP-адрес – уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP.

Malware Information Sharing Platform (MISP) — платформа с открытым исходным кодом для обмена информацией об угрозах ИБ.

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

3. Источники событий

Заказчиком были заявлены и подключены к системе мониторинга Исполнителя следующие хосты:

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	geoportal-zabbix.e-sqo.local	ucta_SKO rev. 35	0.37 %	233 MB	34 seconds ago	8.17.4 Upgrade available	
Healthy	replica-db	ucta_SKO rev. 35	0.78 %	234 MB	30 seconds ago	8.17.4 Upgrade available	
Healthy	backup	ucta_SKO rev. 35	0.47 %	211 MB	26 seconds ago	8.17.4 Upgrade available	
Healthy	geoportal-db	ucta_SKO rev. 35	1.32 %	242 MB	1 minute ago	8.17.4 Upgrade available	
Healthy	repo	ucta_SKO rev. 35	0.61 %	219 MB	16 seconds ago	8.17.4 Upgrade available	
Healthy	geoportal-filesrv	ucta_SKO rev. 35	0.66 %	235 MB	31 seconds ago	8.17.4 Upgrade available	
Healthy	graylog	ucta_SKO rev. 35	0.56 %	228 MB	1 minute ago	8.17.4 Upgrade available	
Healthy	geoportal	ucta_SKO rev. 35	2.39 %	282 MB	2 minutes ago	8.17.4 Upgrade available	

Рисунок 2. Подключенные к системе мониторинга хосты Заказчика

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

4. Классификация событий ИБ

События ИБ подразделяются ключевые категории по уровню критичности, с целью своевременного реагирования и принятия соответствующих мер по обеспечению ИБ.

Уровень критичности	Признаки	Примеры инцидентов ИБ
Высокий (4)	Инциденты ИБ, которые приводят к невозможности предоставления услуг/выполнения работ, и (или) потере/модификации критичных* данных, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего критичные* данные.	- Несанкционированный доступ - Эксплуатация уязвимости - Шифровальщик - Вредоносное ПО - Отказ в обслуживании (DoS/DDoS-атака) И т.д.
Средний (3)	Инциденты ИБ, которые приводят к существенному ограничению предоставления услуг/выполнения работ, и (или) потере/модификации данных, не являющихся критичными*, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего данные, не являющихся критичными*.	- Несанкционированный доступ - Шифровальщик - Вредоносное ПО - Отказ в обслуживании (DoS/DDoS-атака) - Эксплуатация уязвимости И т.д.
Низкий (2)	Инциденты ИБ, не влияющие на предоставление услуги/выполнение работ.	- Вредоносное ПО - Отказ в обслуживании (DoS/DdoS-атака) - Эксплуатация уязвимости - Спам - Фишинговая атака И т.д.
Не определено (1)**	Влияние инцидента ИБ на предоставление услуг не определено	Нехарактерная/ подозрительная активность

Следует отметить, что аналитик ОЦИБ имеет полномочия самостоятельного определения уровня критичности, при необходимости, во избежание значительных отрицательных последствий.

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

5. РЕЗУЛЬТАТЫ МОНИТОРИНГА

Исполнитель осуществляет постоянный мониторинг событий ИБ, в отношении подключённой к SIEM информационно-коммуникационной инфраструктуры Заказчика.

Все зарегистрированные, подтвержденные инциденты ИБ направляются в адрес НКЦИБ АО «ГТС» в соответствии с «Правилами обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности» утвержденных Приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НҚ.

За отчетный период ОЦИБ были определены следующие показатели:

- Количество обработанных событий: **349 150 264;**
- Количество зафиксированных событий ИБ: **0.**

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

Рисунок 3. Количество обработанных событий ИБ за отчетный период

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

На рисунке 4 отображено процентное соотношение событий, генерируемых подключенными источниками.

Основная доля (63,42%) событий поступает от хоста geoportal-db.

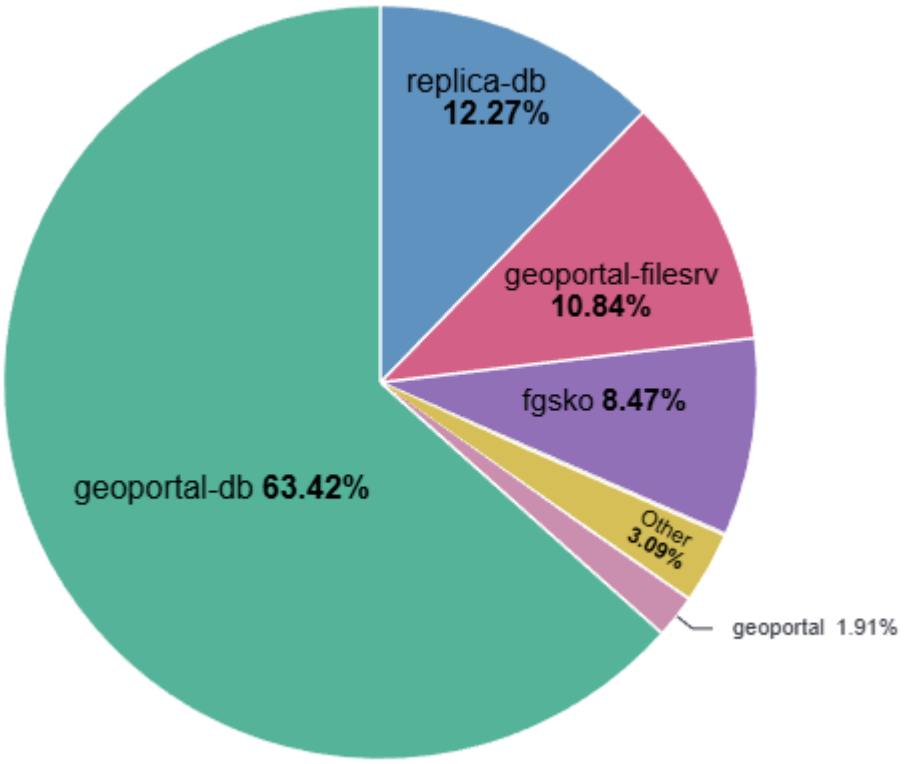

Рисунок 4. Источники, направляющие основную часть событий ИБ

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

6. Рекомендации

Комплекс мер по повышению уровня защищенности информационно-коммуникационной инфраструктуры Заказчика:

1. Запланировать обновление рабочих станций, работающих на операционной системе (ОС) Windows 10 ввиду окончания официальной поддержки указанной версии. Устаревшие ОС несут высокие риски эксплуатации потенциальных новых угроз.
2. Внедрить процесс управления уязвимостями для своевременного устранения уязвимостей в инфраструктуре, при необходимости.
3. Установить график создания резервных копий критически важных производственных систем, при необходимости.
4. Провести проверку корпоративных учетных записей на предмет соблюдения корпоративной парольной политики и соблюдения принципа наименьших привилегий.
5. Внедрить двухфакторную аутентификацию для повышения безопасности пользователей в домене.

Рекомендации, разработанные на основе Threat Intelligence (TI) / данных MISP:

Количество уязвимостей: 3.
Уровень критичности: Critical, High.
Производитель: Cisco Systems, Inc.
Известная эксплуатация: не выявлена.

Краткое описание уязвимостей

CVE-2025-20354 – уязвимость в процессе Java Remote Method Invocation (RMI) продукта Cisco Unified Contact Center Express (Unified CCX). Эксплуатация уязвимости может позволить удалённому неаутентифицированному злоумышленнику загрузить произвольные файлы и выполнить команды с правами root на уязвимой системе.

CVE-2025-20358 – уязвимость в приложении Cisco Unified CCX Editor. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, обойти аутентификацию и получить административные права для создания и выполнения сценариев на сервере Unified CCX.

CVE-2025-20343 – уязвимость в функции обработки RADIUS-запросов Cisco Identity Services Engine (ISE). Эксплуатация уязвимости может

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

позволить удалённому неаутентифицированному злоумышленнику вызвать перезапуск устройства и создать состояние отказа в обслуживании (DoS).

Типы уязвимостей

• Remote Code Execution (RCE);

• Authentication Bypass;

• Denial of Service (DoS).

Затронутые версии и продукты:

Cisco Unified Contact Center Express (Unified CCX):

• 12.5 SU3 и более ранние – исправлено в 12.5 SU3 ES07;

• 15.0 – исправлено в 15.0 ES01.

Cisco Identity Services Engine (ISE):

• 3.4.0, 3.4 Patch 1, 3.4 Patch 2, 3.4 Patch 3 (с включенной опцией Reject RADIUS requests from clients with repeated failures) – исправлено в 3.4 Patch 4.

Рекомендации

Организациям, использующим затронутые версии, рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации.

Дополнительно:

• Для Cisco Unified CCX – обновить до 12.5 SU3 ES07 или 15.0 ES01.

• Для Cisco ISE – обновить до версии 3.4 Patch 4 или отключить настройку Reject RADIUS requests from clients with repeated failures до установки обновления.

• Перезагрузка системы требуется после установки обновления.

Техническая информация

• CVE-2025-20354: CWE-434 (Unrestricted File Upload), вектор атаки: удалённый, права не требуются.

• CVE-2025-20358: CWE-306 (Missing Authentication for Critical Function), вектор атаки: удалённый, права не требуются.

• CVE-2025-20343: CWE-697 (Incorrect Comparison), вектор атаки: удалённый, права не требуются.

• Известных IOC – не выявлено.

• Временные обходные меры для CVE-2025-20343 включают отключение функции Reject RADIUS requests from clients with repeated failures.

Количество уязвимостей: 1.

Уровень критичности: высокий.

Производитель: Microsoft Corporation.

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

Сведения об известной эксплуатации: Да, уязвимость эксплуатируется в дикой среде.

Краткое описание уязвимости

Уязвимость CVE-2025-9491 в компоненте обработки файлов ярлыков (.LNK) в Microsoft Windows. Злоумышленник может создать специально сконструированный файл .LNK, в котором аргументы целевого файла скрыты от обычного просмотра пользователем посредством UI-маскировки. При открытии такого ярлыка от имени текущего пользователя возможен запуск произвольного кода.

Типы уязвимости

• Remote Code Execution (RCE)

• Information Disclosure / UI Misrepresentation (маскировка интерфейса)

Затронутые версии и продукты:

• Microsoft Windows 11 версия 23H2 (10.0.22631.4169) и аналогичные сборки.

• Microsoft Windows – общая фраза «Windows» без указания конкретной версии, но используется ярлык .LNK.

Рекомендации

Организациям, использующим затронутые версии, рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации.

Дополнительные рекомендации:

• ограничить или блокировать открытие файлов .LNK из недоверенных источников;

• мониторить запуски скриптов (PowerShell, CMD) и отслеживать подозрительную активность замаскированных ярлыков;

• контроль DLL side-loading легитимных процессов и анализ исходящих подключений к CloudFront CDN;

• внедрить многоуровневую защиту путем включения современных EDR/AV, использовать Smart App Control и фильтрацию входящих файлов;

• усилить обучение пользователей, не открывать вложения или ссылки из непроверенных писем, особенно от внешних источников.

Техническая информация

• CWE: CWE 451 — UI Misrepresentation of Critical Information.

• Вектор атаки (CVSS 3.x): AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H.

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

• Требуемые привилегии: не требуются (PR:N) — атака возможна от имени текущего пользователя при взаимодействии (UI:R) с файлом.

• Индикаторы компрометации (IOC):

• использование .LNK-файлов с аномально длинным Target полем;

• маскировка аргументов, запуск цепочек через PowerShell;

• DLL-side-loading легитимных подписанных утилит (например, принтер-драйверы Canon, через cnmpaui.exe, cnmpauix.exe, cnmplog.dat) по данным кампании;

• HTA файлы с загрузкой JS с CloudFront URL;

• Инфраструктура C2 на базе CloudFront.

Тип документа: конкретные уязвимости. Количество уязвимостей: 1. Уровень критичности: Critical. Производитель: Squid Project. Известная эксплуатация: не выявлена.

Краткое описание уязвимости CVE-2025-62168 – критическая уязвимость в механизме обработки ошибок кэш-прокси сервера Squid, связанная с утечкой HTTP-аутентификационных данных. Эксплуатация уязвимости может позволить удалённому злоумышленнику получить токены и учетные данные, используемые доверенными клиентами для аутентификации, что создаёт риск несанкционированного доступа к внутренним веб-приложениям и сервисам.

Типы уязвимостей • Information Disclosure; • Credential Exposure.

Затронутые версии: • Все версии Squid до 7.2 включительно (≤ 7.1) Уязвимы системы с параметром email_err_data on в конфигурации. Уязвимы также экземпляры без явного включения HTTP Authentication.

Рекомендации Организациям, использующим затронутые версии, рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации. Дополнительно: • Обновить Squid до версии 7.2 или применить патч 0951a06. • При невозможности немедленного обновления – временно отключить вывод отладочной информации в почтовых ссылках администратора. • После обновления рекомендуется перезапуск службы Squid и проверка конфигурации.

Техническая информация • CWE: CWE-209 (Generation of Error Message Containing Sensitive Information), CWE-550 (Server-generated Error Message Containing Sensitive Information). • Вектор атаки: удалённый, без аутентификации. • Требуемые привилегии: не требуются. • Механизм: утечка

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

HTTP Authentication данных при генерации страниц ошибок. • Обходные меры: email_err_data off – временно устраняет уязвимость до обновления. • IOC: отсутствуют публичные индикаторы компрометации.

Тип документа: «конкретные уязвимости».

Количество уязвимостей: 2.

Уровень критичности: средний / высокий (в зависимости от CVE).

Производитель: Zoho Corp (продукт: ManageEngine Exchange Reporter Plus).

Известная эксплуатация: на момент публикации официальных данных об эксплуатации не подтверждено.

Краткое описание уязвимостей

Уязвимость CVE-2025-5343 связана с модулем «Instant Search» продукта ManageEngine Exchange Reporter Plus. Эксплуатация может позволить злоумышленнику внедрить хранимый (Stored) скрипт (XSS), который позволит через сеть воздействовать на целевое приложение и добиться изменения данных или выполнения нежелательных скриптов.

Уязвимость CVE-2025-5347 затрагивает модуль отчётов (reports module) того же продукта ManageEngine Exchange Reporter Plus. Эксплуатация может позволить злоумышленнику внедрить хранимый скрипт (Stored XSS) и при просмотре отчёта пользователем, выполнить нежелательные действия от имени этого пользователя.

Типы уязвимостей

• Cross-Site Scripting (Stored XSS)

• Improper Neutralization of Input During Web Page Generation (CWE-79)

Затронутые версии и продукты:

• ManageEngine Exchange Reporter Plus — версии до сборки 5721 включительно (для CVE-2025-5343)

• ManageEngine Exchange Reporter Plus — версии до сборки 5723 включительно (для CVE-2025-5347)

Рекомендации

Организациям, использующим затронутые версии, рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации.

Дополнительные рекомендации:

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

• проверить наличие сборки 5722 или выше (для CVE-2025-5343) и/или сборки 5723 или выше (для CVE-2025-5347) продукта ManageEngine Exchange Reporter Plus;

• перезагрузить сервис после установки обновления (если рекомендовано производителем);

• ограничить права пользователей, имеющих доступ к функциям Instant Search и модулям создания/просмотра отчётов, до минимально необходимых;

• внедрить проверку входных данных (input validation) и кодирование/экранирование вывода (output encoding/escaping) в пользовательских полях, до момента выхода обновления;

• настроить мониторинг логов приложения на попытки выполнения скриптов и аномалии активности в модулях Instant Search и reports;

• использовать Web Application Firewall (WAF) с блокировкой подозрительных скриптов

Техническая информация

• CWE: 79 – Improper Neutralization of Input During Web Page Generation.

• Вектор атаки: сетевой (AV:N)

• Требуемые привилегии: пользователь с правами низкого уровня (например, обычный пользователь приложения) способен инициировать запрос, допускающий хранение вредоносного скрипта.

• Индикаторы компрометации (IOC): участие неизвестных скриптов или тегов в полях Instant Search или отчётов; увеличение числа запросов с подозрительными параметрами; аномальная активность пользователей при просмотре отчётов.

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

7. Заключение

В рамках оказания услуг в заведенной за мониторинг информационно-коммуникационной инфраструктуре Заказчика в ноябре 2025 года инциденты ИБ не зафиксированы.

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z1202500001700112B9EF
Тип документа	Исходящее письмо
Тема	отчеты за ноябрь 2025 года. пароль передан исполнителю
Статус	Доставлен
Рег. Номер:	01-01/618
Рег. Дата:	03.12.2025
Количество страниц	17
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	109.163.197.162

Информация о получателях

Получатель 1	КГУ «Управление цифровых технологий акимата Северо-Казахстанской области» , 055421500000, Казахстан

Информация о подписантах

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Заместитель Генерального директора
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWFQYJ...hO9LX+VA=
Дата подписания	03.12.2025 12:51

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Заместитель Генерального директора
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWTAYJ...3Jq1X4a4I

Дата подписания 03.12.2025 12:51

DOC ID KZBW2Z1202500001700112B9EF

DOC ID KZBW2Z1202500001700112B9EF
Электронный документ подписан в Documentolog Business