|  |  |  |
| --- | --- | --- |
| **СОГЛАСОВАНО**  Главный инженер – первый заместитель генерального директора ООО «Газпром информ»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.В. Манюков |  | **УТВЕРЖДАЮ**  Заместитель  генерального директора  по специальным работам  ООО «Газпром информ»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ю.Н. Гвоздёв |
| «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г. |  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г. |

**Сценарий реагирования**

**на события, связанные с успешной аутентификацией под встроенной учетной записью**

ЛИСТ СОГЛАСОВАНИЯ

к Сценарию реагирования на события, связанные с успешной

аутентификацией под встроенной учетной записью

|  |  |  |  |
| --- | --- | --- | --- |
| **Должность** | **Дата** | **Подпись** | **ФИО** |
| Начальник Управления контроля эффективности мер защиты информации |  |  | А.В. Смирнов |
| Начальник Управления эксплуатации информационно-вычислительной инфраструктуры |  |  | А.В. Кинев |
| Начальник Управления защиты информационных систем |  |  | М.Б. Баранов |
| Начальник Управления эксплуатации системных ландшафтов |  |  | В.В. Зубко |

# список СОКРАЩЕНИй

| **Сокращение** | **Определение** |
| --- | --- |
| АИБ | Администратор информационной безопасности |
| АСО | Активное сетевое оборудование |
| ДС УКЭМЗИ | Дежурная смена Управления контроля эффективности мер защиты информации |
| ИАС КСУИБ | Информационно-аналитическая система корпоративной системы управления информационной безопасностью |
| ИВС | Информационно-вычислительная сеть администрации ПАО «Газпром» |
| ИУС | Информационно-управляющая система |
| МЭ | Межсетевые экраны |
| НКЦКИ | Национальный координационный центр по компьютерным инцидентам |
| ОС | Операционная система |
| ОЭВК | Отдел эксплуатации вычислительных комплексов |
| ПО | Программное обеспечение |
| ППО | Прикладное программное обеспечение |
| СКЗ | Служба корпоративной защиты ПАО «Газпром» |
| СУБД | Системы управления базами данных |
| УКЭМЗИ | Управление контроля эффективности мер защиты информации |
| УЗ | Учетная запись |
| УЗИС | Управление защиты информационных систем |
| УЭИВИ | Управление эксплуатации информационно-вычислительной инфраструктуры |
| УЭСЛ | Управление эксплуатации системных ландшафтов |
| ЦКБ | Центр кибербезопасности Службы корпоративной защиты ПАО «Газпром» |
| ЦОД-М | Центр обработки данных «Москва» |

Данный документ предназначен для определения перечня действий и порядка взаимодействия структурных подразделений Общества, ответственных за сопровождение ИТ-активов, расположенных на системно-технической инфраструктуре Центра обработки данных ПАО «Газпром» и Информационно-вычислительной системы администрации ПАО «Газпром», при реагировании на события информационной безопасности.

Под встроенной учетной записью в контексте данного документа понимается техническая (сервисная, служебная) учетная запись, используемая в технологических процессах работы инфраструктуры или встроенных производителями программных (программно-аппаратных) средств в такие средства, а также учетная запись администратора программных (программно-аппаратных) средств.

При получении событий от SIEM на электронную почту ДС УКЭМЗИ или в консоль R-Vision, связанных с успешной аутентификацией на операционные системы, СУБД или ППО под встроенной учетной записью, выполняются следующие мероприятия:

* 1. Определение принадлежности объекта защиты[[1]](#footnote-1) к ИТ-активу, в отношении которого выявлено нарушение, связанное с успешной аутентификацией под встроенной учетной записью. Идентификация пользователя (Ф.И.О. работника Общества, его учётная запись), осуществившего аутентификацию под встроенной учетной записью, идентификация объекта защиты (наименование сервера/хоста/базы данных, его IP-адрес). Проверка наличия запланированных работ в ИТ-календаре или оповещения по электронной почте. ***Ответственный – ДС УКЭМЗИ.***
  2. Выполнение мероприятий по первичному реагированию:
  3. Если аутентификация под встроенной учетной записью (далее - аутентификация) была выполнена в рамках запланированных работ, отраженных в ИТ-календаре, или присутствует оповещение по электронной почте от администраторов объектов защиты, или связана со штатной работой системы (включая работу легитимных скриптов администраторов), или система находится в стадии разработки/опытной эксплуатации, то дальнейшие действия не выполняются. ***Ответственный – ДС УКЭМЗИ.***
  4. Если аутентификация была выполнена в рамках работ, которые не были отражены в ИТ-календаре, или не было оповещения по электронной почте от администраторов объектов защиты, или учетная запись не соответствует проектным решениям, направляется запрос администраторам объектов защиты (ответственным за УЗ) по электронной почте и телефону, в отношении которых выявлены факты нарушений, связанные с аутентификацией. В случае, если использование встроенной учетной записи в рамках проведения работ на объектах защиты подтверждено администраторами:
* передача информации о факте нарушения в адрес АИБ ИТ-актива. ***Ответственный – ДС УКЭМЗИ.***
* запрос объяснительной записки от виновного должностного лица (администратора объекта защиты или его руководителя) по факту установленного нарушения. ***Ответственный – АИБ ИТ-актива.***
* Предоставление скан-копии объяснительной записки в течение двух дней по факту нарушения аутентификации в адрес АИБ ИТ-актива. ***Ответственный – администратор объекта защиты (ответственный за УЗ) или его руководитель[[2]](#footnote-2).***
  1. Если аутентификация (пользователь, который не несёт ответственность за учетную запись – «злоумышленник») произведена несанкционированно (по каким-либо признакам выявлено отклонение от нормы выполняемых задач под данной УЗ или наблюдается аномальная активность на том же объекте защиты), осуществляется информирование в установленном порядке ответственных лиц Общества и ЦКБ. Создание карточки инцидента в ИАС КСУИБ. ***Ответственный – ДС УКЭМЗИ.***

3. Выполняются мероприятия по установлению причин и обстоятельств по факту нарушения аутентификации, а также по предотвращению возможных последствий данной аутентификации:

3.1. Блокировка учетной записи и принудительное завершение сеанса пользователя. ***Ответственный*** *–* ***администратор объекта защиты***.

3.2. Изъятие файлов логирования, содержащих события информационной безопасности и направление их в УКЭМЗИ. ***Ответственный – администратор объекта защиты.***

3.3. Проведение антивирусной проверки средством антивирусной защиты источника, на который была произведена несанкционированная аутентификация (при возможности).

3.4. Проведение разбирательства по факту выявленного нарушения и выяснение масштаба нанесенного ущерба. ***Ответственный – УКЭМЗИ, а также другие подразделения (например, УЭИВИ, УЗИС, УЭСЛ), участвующие в сопровождение объекта защиты.***

4. В случае выявления деструктивного воздействия на объектах защиты по результатам анализа материалов – устранение его последствий. Информирование УКЭМЗИ об устранений последствий. ***Ответственный – администратор объекта защиты****.*

5. Заполнение обязательных полей в карточке инцидента ИАС КСУИБ и установка статуса «отработан». ***Ответственный – УКЭМЗИ***.

*Справочно: в карточке инцидента необходимо обязательно заполнить поля «Причина инцидента», «Результат отработки инцидента» (после выставления статуса «отработан» в поле «Статус отработки ДО»).*

6. Закрытие карточки инцидента в ИАС КСУИБ. ***Ответственный – ЦКБ***.

Приложение

к Сценарию реагирования на событиям, связанные

с успешной аутентификацией под встроенной учетной записью

**КОНТАКТНАЯ ИНФОРМАЦИЯ**

**для информирования должностных лиц,**

**участвующих в процессе реагирования на события,**

**связанные с успешной аутентификацией под встроенной учетной записью**

|  |  |  |  |
| --- | --- | --- | --- |
| **ЦКБ** | | | |
|  | Отдел мониторинга и взаимодействия с НКЦКИ | Monitoring.sb@ss.gazprom.ru | (700) 4-12-52  (общий) |

**Взаимодействия в Обществе по электронной почте осуществляются с работниками, представленными в следующей таблице:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия Имя Отчество** | **Электронная почта** | **Телефон** |
| **УКЭМЗИ** | | | |
|  | Группа мониторинга событий информационной безопасности отдела мониторинга УКЭМЗИ | DL\_UKEMZI@inform.gazprom.ru | (700) 5-97-29 |
|  | Администраторы ИБ | aib@inform.gazprom.ru | (700) 2-03-16 |
|  | Боровков Андрей Владимирович | a[.borovkov@inform.gazprom.ru](mailto:a.borovkov@inform.gazprom.ru) | (700) 2-01-68 |
|  | Горбунов Борис Вячеславович | b.gorbunov@inform.gazprom.ru | (700) 2-03-28 |
|  | Колошин Андрей Петрович | a.koloshin@inform.gazprom.ru | (700) 2-03-16 |
|  | Жуков Роман Вячеславович | r.jukov@inform.gazprom.ru | (700) 2-04-32 |
| **УЗИС** | | | |
|  | Казаков Евгений Валерьевич | E.Kazakov@inform.gazprom.ru | (700) 9-84-10 |
|  | Баранов Михаил Борисович | [M.Baranov@inform.gazprom.ru](mailto:M.Baranov@inform.gazprom.ru) | (700) 9-22-04 |
| **УЭИВИ** | | | |
| **ОЭВК** | | | |
|  | Сапрыкин Виктор Иванович | [v.saprykin@inform.gazprom.ru](mailto:v.saprykin@inform.gazprom.ru) | (700) 9-85-72 | |
|  | Скоморохов Владимир Александрович | [v.a.skomorokhov@inform.gazprom.ru](mailto:v.a.skomorokhov@inform.gazprom.ru) | (700) 4-44-97 | |
|  | Огай Юрий Дмитриевич | [y.ogay@inform.gazprom.ru](mailto:y.ogay@inform.gazprom.ru) | (700) 9-55-62 | |
|  | Ковальчук Олег Дмитриевич | [o.kovaltchuk@inform.gazprom.ru](mailto:o.kovaltchuk@inform.gazprom.ru) | (700) 9-55-63 | |
| **В части ОС Windows Server (в Москве):** | | | | |
|  | Группа рассылки ОЭОПО УЭИВИ | dl\_oeopo@inform.gazprom.ru | (700) 9-50-37 | |
|  | Минин Алексей Владимирович | a.minin@inform.gazprom.ru | (700) 9-50-37 | |
|  | Сиротин Павел Александрович | p.sirotin@inform.gazprom.ru | (700) 9-45-69 | |
| **В части ОС Windows Server (в Санкт-Петербурге):** | | | |
|  | Новиков Александр Александрович | a.a.novikov@inform.gazprom.ru | (700) 2-18-86 |
|  | Коршунов Данила Сергеевич | d.korshunov@inform.gazprom.ru | (700) 2-18-85 |
| **В части СУБД**: | | | |
|  | Мартыненков Александр Николаевич | [a.martynenkov@inform.gazprom.ru](mailto:a.martynenkov@inform.gazprom.ru) | (700) 5-90-85 |
|  | Богданова Евгения Александровна | [e.bogdanova@inform.gazprom.ru](mailto:e.bogdanova@inform.gazprom.ru) | (700) 9-50-07 |
| **УЭСЛ** | | | |
| **В части ППО SAP:** | | | |
|  | Кочетков Вадим Николаевич | [v.kotchetkov@inform.gazprom.ru](mailto:v.kotchetkov@inform.gazprom.ru) | (700) 9-33-64 |
|  | Гапоненко Андрей Юрьевич | a.gaponenko@inform.gazprom.ru | (700) 9-53-81 |

1. Под объектами защиты понимается ПО в составе ИТ-актива, выполняющего функции по защите информации в соответствии с проектными решениями. [↑](#footnote-ref-1)
2. Работник ООО «Газпром информ», ответственный за сопровождение и эксплуатацию типовых объектов защиты ИТ-активов ПАО «Газпром» и ООО «Газпром информ» в соответствии с приказом АБ-251 от 26.08.2022г. [↑](#footnote-ref-2)