УДК 004

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЧЕСКОЙ ПЛАТФОРМЫ «1С: ПРЕДПРИЯТИЕ» ДЛЯ АВТОМАТИЗАЦИИ УЧЁТА И УВЕДОМЛЕНИЯ ГОССОПКА ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Хохлов А.Ю., студент гр. ИТб-201, IV курс
Асанов С.А., старший преподаватель кафедры информационных и автоматизированных производственных систем
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кузбасский государственный технический университет имени Т.Ф. Горбачёва»
г. Кемерово

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее — ГосСОПКА) — созданный на основе Указа Президента РФ №31с от 15.01.2013 единый комплекс, включающий в себя как программные, так и технические инструменты для обнаружения, предупреждения и ликвидации последствий компьютерных и информационных атак на информационные ресурсы Российской Федерации.

Каждый владелец объектов критической информационной инфраструктуры (далее — КИИ), должен информировать НКЦКИ с помощью данной системы о любых инцидентах и компьютерных атаках на информационные ресурсы.

Существует несколько категорий значимости объектов КИИ:

1. Объект первой категории;
2. Объект второй категории;
3. Объект третьей категории;
4. Объект КИИ без категории;
5. Информационный ресурс не является объектом КИИ.

Для каждой категории были определены соответствующие рамки, в которые необходимо попасть для её присваивания объекту, так же данные рамки различаются от сферы функционирования объекта. Подробный перечень показатель критериев значимости определён Постановлением Правительства от 8 февраля 2018 №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Направление уведомления в ГосСОПКА определяется правилами, установленными на совещании НКЦКИ следующего содержания:

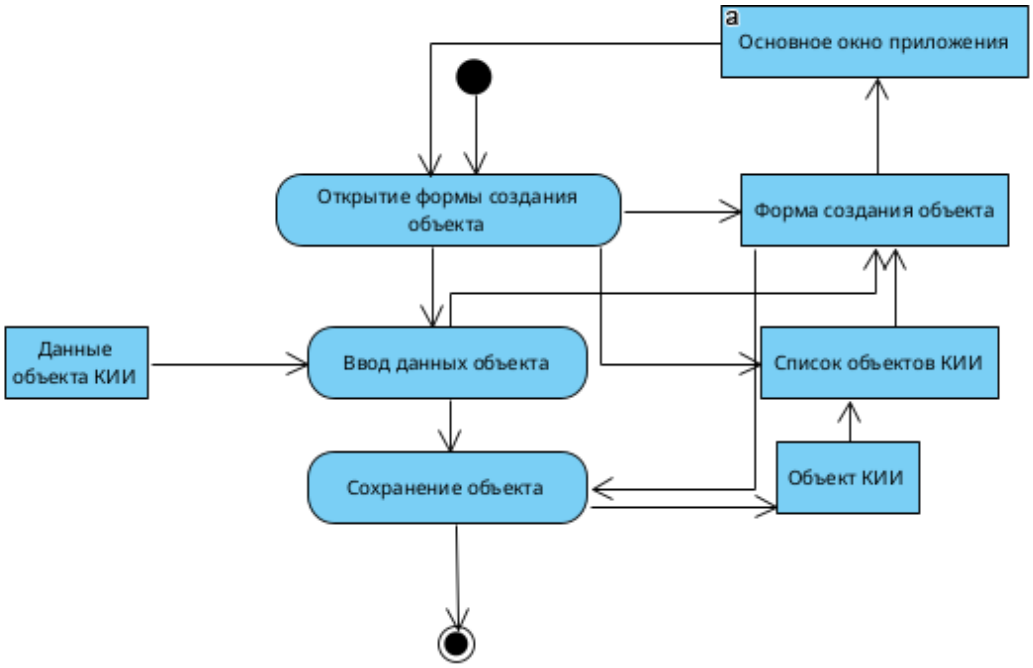
1. Разбиения на этапы процесса формирования уведомления;

2. Разделение всех уведомлений на категории и соответствующие им типы событий ИБ;
3. Составление шаблонов формирования уведомления для каждого типа события ИБ;
4. Разбиение шаблонов на блоки и содержащиеся в них сведения;
5. Заполнение полей блоков;
6. Формирование инструкции по направлению уведомлений.

Однако не все предприятия ведут оперативный учёт и информируют НКЦКИ. Множество уведомлений составляются с задержкой, когда вредное влияние на объект КИИ завершилось или вовсе вывело из строя информационный ресурс.

Устранить подобные издержки времени и рабочей силы призван программный продукт от «1С» - «1С: Предприятие». Он позволяет автоматизировать деятельность сотрудников на предприятии и его бизнес-процессы, вести удобный и эффективный учёт и документооборот.

В ходе анализа уже составленной НКЦКИ инструкции по формированию электронного письма-уведомления о компьютерном инциденте, атаке или уязвимости были выделены следующие сущности для автоматизации:



- Информационный ресурс или же объект КИИ;

Рисунок 1 — Диаграмма деятельностей для ввода в эксплуатацию уже существующего информационного ресурса

- Событие ИБ или же компьютерный инцидент или событие;

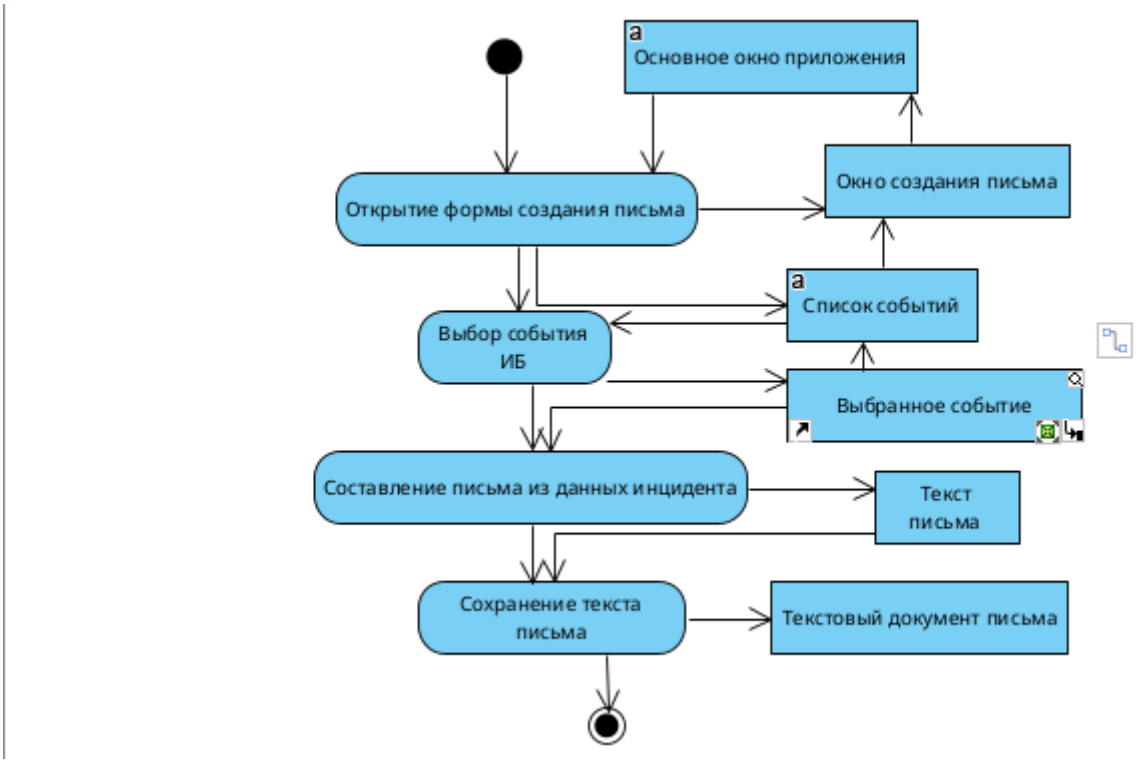
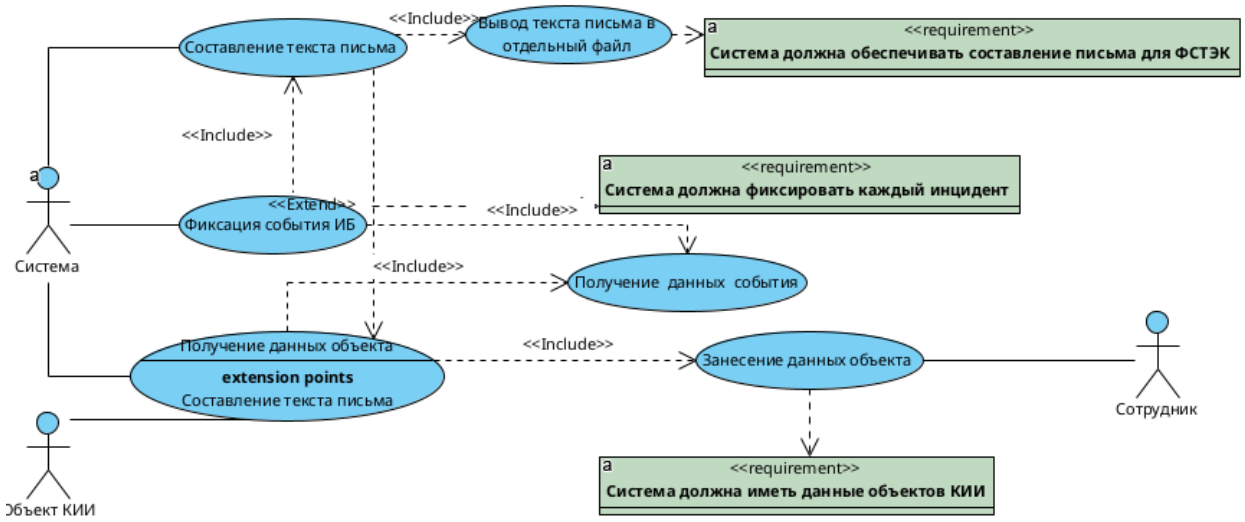


Рисунок 2 — Диаграмма деятельностей для составления письма-



уведомления

Рисунок 3 — Диаграмма вариантов использования системы

Определившись с составом системы следует занести его в конфигурацию — основу нашей системы: поскольку «Событие ИБ» является отчётной сущностью, его следует занести в Документы — главный прикладной объект конфигурации.

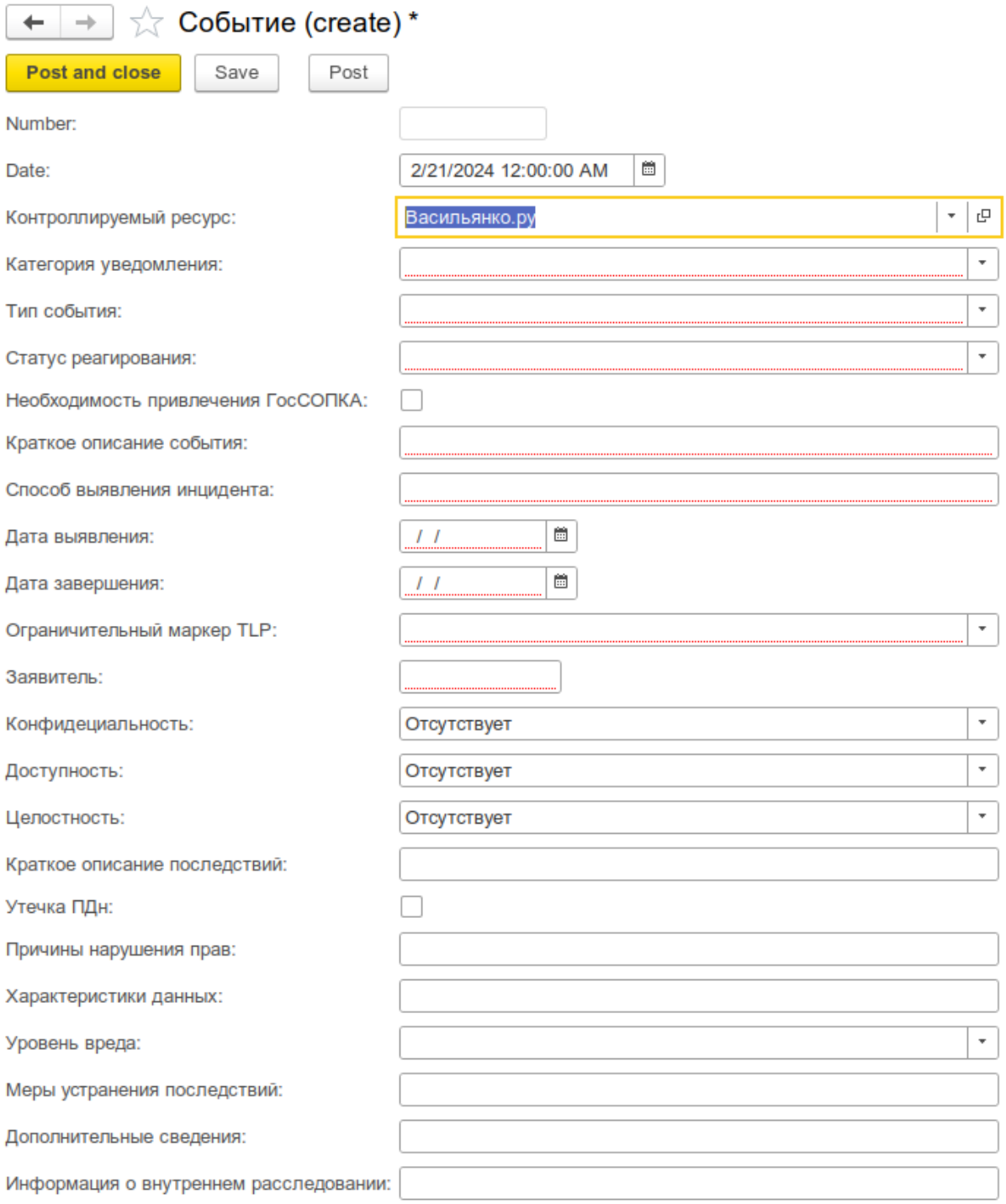


Рисунок 4 — Окно создания события

Далее создадим следующую основную сущность - «Объект КИИ», о событии которого составляется письмо-уведомление.

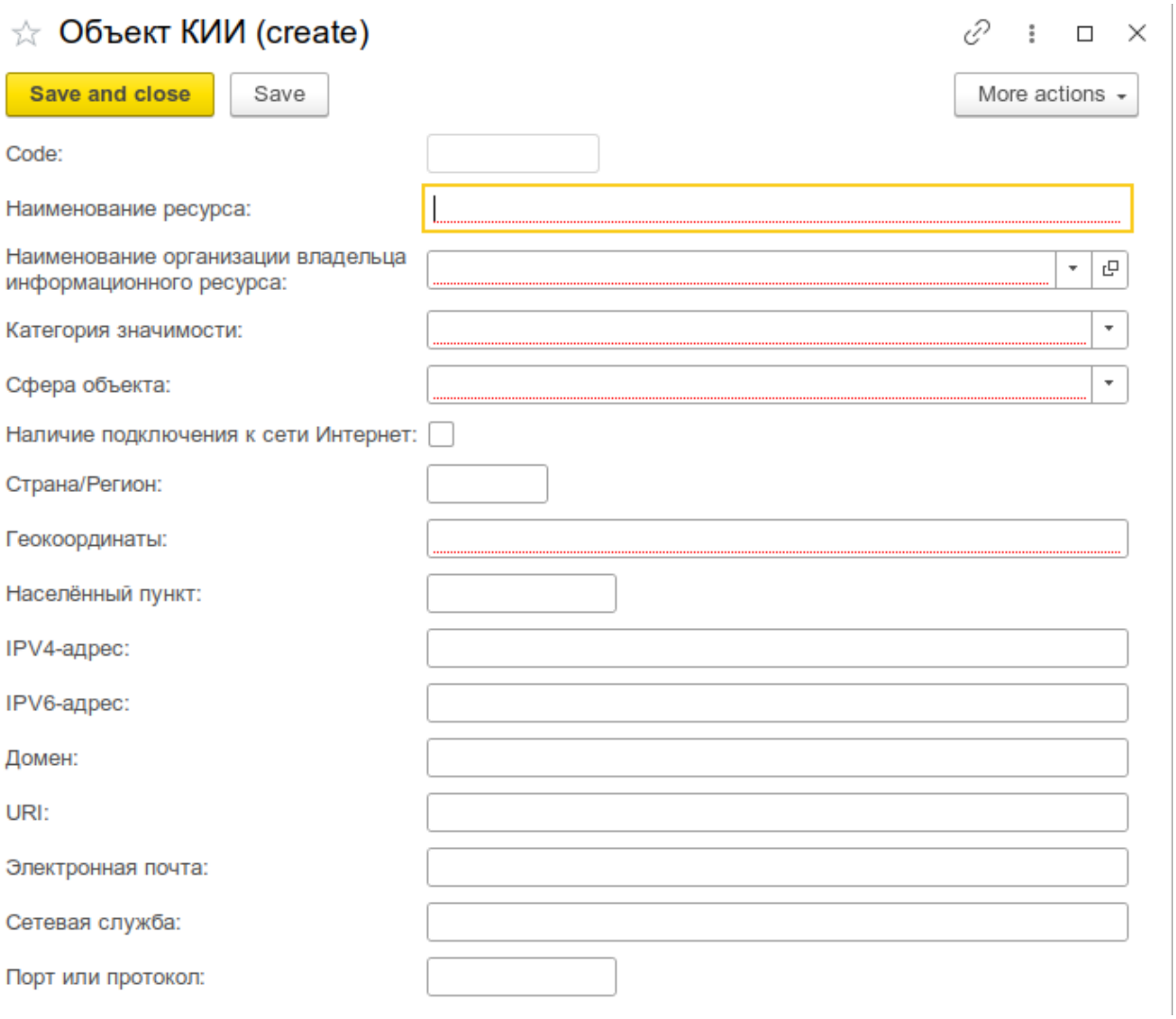


Рисунок 5 — Окно создания Объекта

Во время атаки на информационный ресурс сотрудник заполняет кортеж события и формирует текстовый документ сообщения в ГосСОПКА:

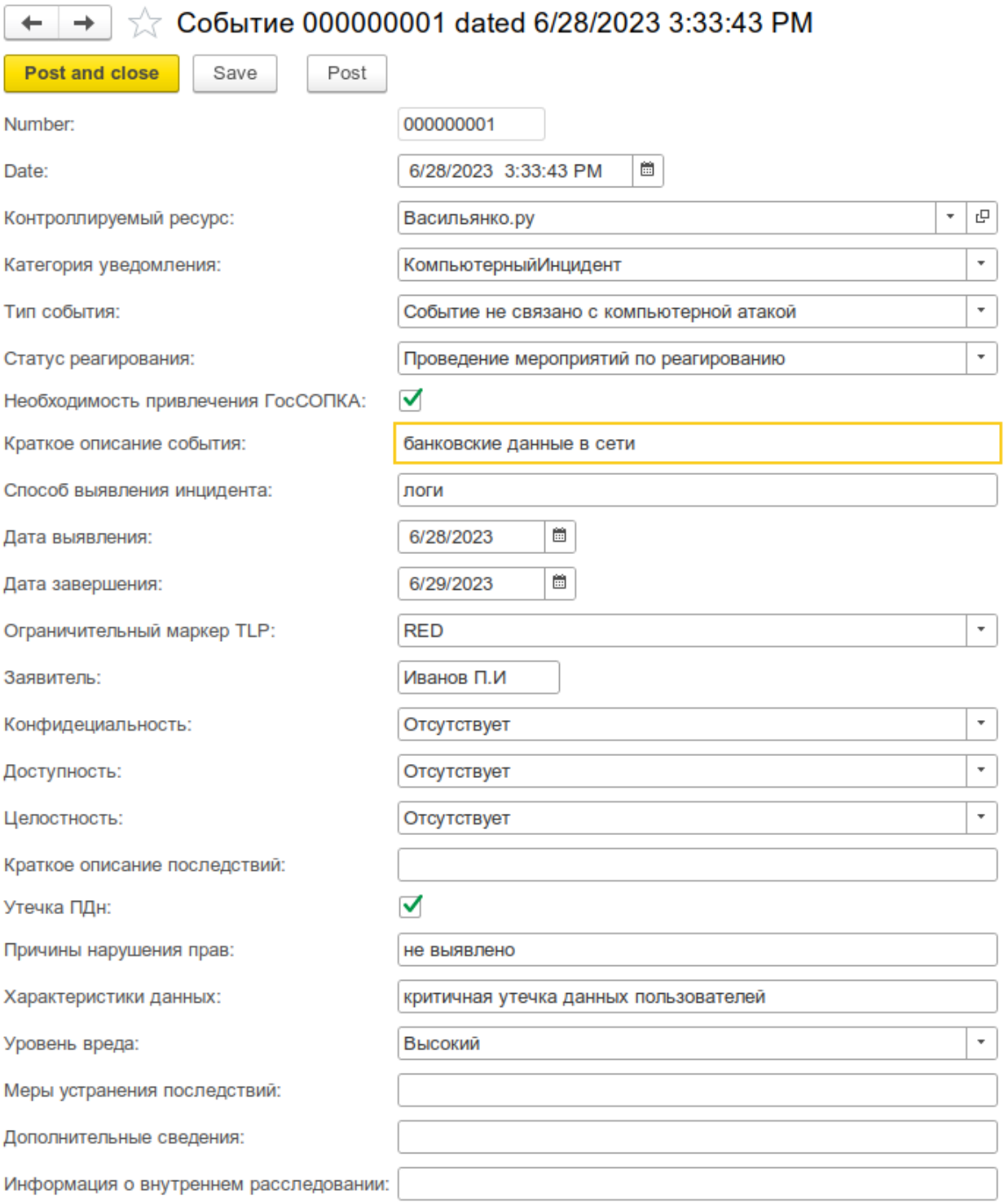


Рисунок 6 — Заполненный кортеж «События»

```
   Событие не связано с

Номер    : 000000001
Дата     : 6/28/2023
Объект   : Васильянко.ру
Общие сведения:

    Наименование организации владельца информационного ресурса ПАО "Эхехео"
    Категория: КомпьютерныйИнцидент
    Тип события ИБ: Событие не
    Статус реагирования: Проведение мероприятий по
    Необходимость привлечения сил ГосСОПКА: Yes
    Краткое описание события ИБ: банковские данные в
    Сведения о средстве или способе выявления: логи
    Дата и время выявления: 6/28/2023 12:00:00 AM
    Дата и время завершения: 6/29/2023 12:00:00 AM
    Ограничительный маркер TLP: RED
    Заявитель: Иванов П.И
    Влияние на конфиденциальность: Отсутствует
    Влияние на целостность: Отсутствует
    Влияние на доступность: Отсутствует
    Краткое описание иной формы последствий компьютерного инцидента:
    Утечка ПДн: Yes

Общие сведения о контроллируемом ресурсе:

    Наименование: Васильянко.ру
    Информация о категорировании ОКИИ: Ресурс признан не значимым
    Сфера функционирования: Банковская
    Наличие подключения к сети Интернет: Yes

Местоположение контролируемого ресурса:

    Локация: NSK
    Населенный пункт или геокоординаты: ХЗ


Технические сведения об атакованном/уязвимом ресурсе:

    IPv4-адрес: 45.232.23.11
    IPv6-адрес: 0bda:ffa1:17b0:000f
    Доменное имя:
    URI-адрес:
    Email-адрес атакованного ресурса:
    Сетевая служба и порт/протокол:                          ,

Технические сведения о вредоносной системе:


Сведения об утечке персональных данных

    ИНН: 4,002,145,555
```

Рисунок 7 — Отрывок сформированного текстового документа-сообщения

Благодаря разработанной системе информировать ГосСОПКа стало проще, достаточно заполнить атрибуты события и отправить сформированный документ по почте.

Список использованной литературы:

1. Указ Президента РФ №31с от 15.01.2013;
2. ПП от 8 февраля 2018 №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
3. Инструкция по формированию электронного письма уведомления о компьютерном инциденте, атаке или уязвимости от 05.05.2023.