Пример заполненной типовой формы отчета о проведении мероприятий

По результатам проводимых работ в период с 28 июня по 5 августа 2021 года специалисты «____» (далее - Исполнитель) провели работы по верификации недопустимых событий (далее – НС) в отношении «____» (далее - Заказчик).

1. Экспертная оценка уровня защищенности периметра: крайне низкий, низкий, средний, высокий (где крайне низкий – наличие общеизвестной уязвимости с возможностью удаленного выполнения кода (RCE))
Средний – обнаружено использование небезопасных сервисов на периметре (SMB, HP iLO), обнаружено множество доменов с просроченными сертификатами, а также домены с самоподписанными сертификатами.
2. Общее количество исследуемых НС, количество реализованных НС
НС – 20; Реализованных НС - 4.
3. Реестр реализованных НС (подтверждение, длительность, квалификация)
1. «Утечка персональных данных граждан и другой информации конфиденциального характера»: частичная верификация, 12 суток, низкая квалификация. 2. «Нарушение процесса оказания государственных услуг по причине неработоспособности веб-ресурсов в результате кибератаки»: полная верификация, 18 суток, низкая квалификация. 3. «Мошеннические действия в банковских системах с использованием скомпрометированной цифровой личности пользователя: полная верификация, 27 суток, низкая квалификация. 4. «Мошенничество в адрес пользователей путем подмены отображаемых на сайте данных»: частичная верификация, 11 суток, средняя квалификация.
5. Перечень ограничений, наложенных в рамках реализации работ
Организационные: отсутствие согласования проведения работ в выходные дни. Технические: приостановка работ с 10 по 15 июля 2021 года.
6. Противодействие со стороны Заказчика
Принятые меры: отключены веб-приложение, заблокированы сетевые подключения специалистов Исполнителя. Эффективность: меры по противодействию, предпринятые сотрудниками службы безопасности, оказались неэффективными.
7. Резюме Исполнителя с указанием квалификации сотрудников
30 квалифицированных специалистов по практической кибербезопасности в штате компании. 100 проектов по тестированию на проникновение и анализу защищенности приложений успешно выполнено. Сертификаты: OSCP, OSWE, GPEN, GWAPT, CISSP, CISM, CRISC, CISA, CEH.
8. Описание целей и сроков последующей оценки защищенности
Сроки проведения: 1 квартал 2023 года Планируемый % покрытия информационной инфраструктуры: 100% Планируемый % покрытия НС: 100%
9. Выводы о результатах проведения работ по оценке уровня защищенности (не более 250 слов)
Обнаружен ряд уязвимостей в ПО на сетевом периметре и во внутренней инфраструктуре, обнаружен вектор проникновения в ЛВС, который стал недоступен из-за оперативного вмешательства службы безопасности Заказчика. Все недопустимые события верифицированы полностью или частично. При этом был предоставлен физический доступ к ЛВС, без которого указанные цели достигнуты бы не были.

10. Подписи ответственных лиц		
Заместитель генерального директора АО «Заказчик»:	XX.XX.20XX	_____ /ФИО
Генеральный директор АО «Исполнитель»:	XX.XX.20XX	_____/ФИО
Главный эксперт АО «Исполнитель»:	XX.XX.20XX	_____ /ФИО