|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

**ГК/договор None, дата None**

2023-07-31 - 2023-08-23 (при наличии)

**ОТЧЕТ**

**по результатам оказания услуг по анализу защищенности следующих информационных(-ой) систем(-ы)/ЦОД/офис(-ов): customer1**

**Заказ № Пусто** (при наличии)

**Оглавление**

[1 Аннотация 3](#_Toc132983557)

[2 Общие сведения, определения 4](#_Toc132983558)

[3 Границы проведения анализа 6](#_Toc132983559)

[4 Оценка общего уровня защищенности 7](#_Toc132983560)

[5 Выявленные уязвимости объекта анализа защищенности 8](#_Toc132983561)

[6 Аналитические выводы о существующих угрозах и выявленных недостатках конфигурации объекта анализа защищенности 10](#_Toc132983562)

[7 Описание проведенного анализа защищенности 11](#_Toc132983563)

[8 Подробное описание результатов и рекомендации по устранению всех выявленных недостатков 15](#_Toc132983564)

[**8.1** **${Наименование информационной системы/офиса/ЦОД 1}** 15](#_Toc132983565)

[**8.1.1** **${Наименование объекта (url/имя сервера/наименование оборудования) и (или) IP-адрес объекта локальный/белый}** 15](#_Toc132983566)

[**8.2** **${Наименование информационной системы/офиса/ЦОД 2}** 16](#_Toc132983567)

[**8.2.1** **${Наименование объекта (url/имя сервера/наименование оборудования) и (или) IP-адрес объекта локальный/белый}** 16](#_Toc132983568)

# **Аннотация**

Настоящий отчет содержит информацию о результатах выполнения процедуры анализа защищенности Информационных Систем: ; и Офисов/ЦОД: customer1 (далее – Система(ы)) с использованием Ellipsis. Основной целью анализа защищенности являлось выявление уязвимостей Систем(ы), а также уязвимостей, связанных с недостатками их конфигурации.

# **Общие сведения, определения**

При проведении анализа защищенности Исполнитель имитировал действия потенциального внешнего и внутренного нарушителя.

(Далее выбрать одно или несколько из следующих описаний нарушителя)

**Внутренний нарушитель** обладает санкционированным доступом к сети организации и, возможно, штатным доступом к объекту анализа Заказчика, защищенность которого необходимо проанализировать, а также располагает информацией о диапазоне IP-адресов, физическом месторасположении, идентификаторах беспроводной сетей и другими аналогичными сведениями;

**Внешний нарушитель** действует через сеть Интернет и знает только название организации Заказчика и наименование Систем(ы).

**Угрозы безопасности информации**

Под угрозой безопасности информации (Угроза, Риск) понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения целостности, доступности и конфиденциальности информации.

В рамках выполнения работ Исполнитель учитывал существующие условия и факторы, связанные с реализаций и функционированием ИТ-инфраструктуры и систем защиты информации Заказчика, а также новые (перспективные) условия и (или) факторы.

В качестве нарушений безопасности рассматриваются:

* нарушение конфиденциальности, целостности и (или) доступности путем получения несанкционированного доступа к внутрикорпоративной информации, в том числе содержащей ограничительные грифы и (или) пометки (например, «Коммерческая тайна», «Конфиденциально», «Для внутреннего пользования» и т. п.), а также к аутентификационной информации (пароли, закрытые ключи шифрования и т.п.);
* нарушение доступности отдельных информационно-вычислительных ресурсов, оборудования и (или) целых автоматизированных информационных систем Заказчика путем получения контроля (соответствующих прав доступа) над данными ресурсами;
* нарушение неотказуемости путем выполнения значимых действий от имени реальных субъектов доступа.

Ограничениями, принимаемыми при анализе возможности реализации угроз безопасности информации, выступают следующие допущения:

* методика реализации угрозы безопасности информации опубликована в открытых и (или) условно открытых источниках;
* необходимые для реализации угрозы безопасности информации технические средства находятся в свободном доступе и могут быть свободно приобретены.

Под нарушителем понимается только физическое лицо, преднамеренно совершающее действие, следствием которого является нарушение безопасности информации.

При проведении работ предполагается, что нарушитель обладает квалификацией, сравнимой с квалификацией специалистов Исполнителя, имеет доступ к тем же опубликованным методикам выявления и эксплуатации уязвимостей, к которым могут иметь доступ специалисты Исполнителя.

# **Границы проведения анализа**

Согласно полученной от Заказчика информации по объекту анализа, а также информации, полученной в результате проведения Исполнителем пассивного и активного сбора информации и ее изучения, Исполнитель предлагает следующие границы проведения анализа при оказании услуги (таблица 2).

Таблица 2 – Границы анализа

| № ресурса | Указатель ресурса, URL | Адрес ресурса, IP-адрес |
| --- | --- | --- |
| ${Наименование информационной системы/офиса/ЦОД 1} | | |
|  | ${Наименование объекта (url\имя сервера\наименование оборудования} | ${IP-адрес объекта локальный/белый} |
| ${Наименование информационной системы/офиса/ЦОД 2} | | |
|  | ${Наименование объекта (url\имя сервера\наименование оборудования} | ${IP-адрес объекта локальный/белый} |
|  | ${Наименование объекта (url\имя сервера\наименование оборудования} | ${IP-адрес объекта локальный/белый} |

Границы Анализа распространяются на все узлы кластера соответствующего ресурса, в случае если ресурс являются кластерными.

# **Оценка общего уровня защищенности**

Ключевым результатом анализа защищенности по методу blackbox (1 уяз.), blackbox (0 уяз.), blackbox (0 уяз.) является наличие/отсутствие уязвимостей и недостатков, что свидетельствует о недостаточном/ достаточном уровне организации и реализации разработки и эксплуатации.

# **Выявленные уязвимости объекта анализа защищенности**

По результатам выполнения анализа защищенности были обнаружены уязвимости уровней риска, которые могут использоваться злоумышленником для развития атаки и повлиять на общий уровень защищенности. Общая сводка по результатам проведения анализа представлена в таблице 3.

Таким образом, общий уровень защищенности Систем(ы) оценивается как critical.

Таблица 3 – Общая сводка по результатам проведения анализа

|  |  |
| --- | --- |
| Обнаружено уязвимостей | |
| Всего | Ellipsis |
| Критический уровень риска | Ellipsis |
| Высокий уровень риска | Ellipsis |
| Средний уровень риска | Ellipsis |
| Низкий уровень риска | Ellipsis |
| Уровень риска не определен | Ellipsis |
| Информационные сообщения | Ellipsis |

(таблицы далее будут присутствовать только при наличии в отчете нескольких информационных систем/офисов/ЦОД)

Сводка по результатам проведения анализа для каждой(ого) Ellipsis представлена в таблицах Ellipsis.

Таблица ${номер} – Сводка по результатам проведения анализа ${информационной системы/офиса/ЦОД 1}

|  |  |
| --- | --- |
| Обнаружено уязвимостей | |
| Всего | Ellipsis |
| Критический уровень риска | Ellipsis |
| Высокий уровень риска | Ellipsis |
| Средний уровень риска | Ellipsis |
| Низкий уровень риска | Ellipsis |
| Уровень риска не определен | Ellipsis |
| Информационные сообщения | Ellipsis |

Таблица ${номер} – Сводка по результатам проведения анализа ${информационной системы/офиса/ЦОД 2}

|  |  |
| --- | --- |
| Обнаружено уязвимостей | |
| Всего | Ellipsis |
| Критический уровень риска | Ellipsis |
| Высокий уровень риска | Ellipsis |
| Средний уровень риска | Ellipsis |
| Низкий уровень риска | Ellipsis |
| Уровень риска не определен | Ellipsis |
| Информационные сообщения | Ellipsis |

# **Аналитические выводы о существующих угрозах и выявленных недостатках конфигурации объекта анализа защищенности**

По итогам анализа Систем(ы) Исполнитель считает целесообразным обратить внимание специалистов Заказчика на реализацию следующих рекомендаций:

* ${рекомендации к часто встречаемым уязвимостям};
* ${рекомендации к часто встречаемым уязвимостям};
* ...

Более подробные рекомендации по устранению каждой обнаруженной в процессе анализа уязвимости представлены в разделе 8.

# **Описание проведенного анализа защищенности**

(В данном разделе присутствует перечень стандартных инструментов и методик, которые мы пишем для ДИТа. Я думаю, что если оставим их здесь, то ничего страшного и в случае чего в ворде можно будет все поправить, так как в ФАВНе не предусмотрено заведение в БД списка инструментов)

Для проведения инструментального анализа защищенности были использованы следующие средства:

* Acunetix WVS;
* DirBuster;
* BurpSuite Pro;
* w3af;
* Metasploit Framework;
* nse скрипты Nmap;
* Средство анализа защищенности Сканер-ВС;
* Hydra;
* Amass;
* Sqlmap;
* NoSqlMap;
* Cmsmap;
* Wfuzz;
* Ffuf;
* Commix;
* Nessus Professional;
* Bloodhound;
* Встроенные утилиты по работе с СУБД (sqldeveloper, mysql, psql);
* Tplmap;
* NetCat;
* Telnet;
* Встроенные в дистрибутивы Linux веб-клиенты.

(следующий абзац со списком инструментов указывается при наличии ручной верификации уязвимостей)

Для проведения ручного поиска уязвимостей и недостатков, а также их верификации по результатам автоматизированного поиска были использованы следующие средства:

* браузер Mozilla Firefox, с установленными плагинами:
* Live HTTP headers;
* Tamper Data;
* Cookie Manager+;
* Modify Headers;
* Hackbar;
* приложение Burp Suite;
* приложение ProxyStrike.

(далее все указывается в отчете)

Для выявленных уязвимостей проведена оценка уровней риска и выработаны рекомендации по их устранению.

В ходе выполнения работ используются собственные наработки, базирующие на следующих международных практиках OSSTMM, OWASP, WASC и ISECOM.

Эти методики позволяют идентифицировать ряд классов атак и уязвимостей:

* подбор паролей (Brute Force);
* недостаточная аутентификация/авторизация (Insufficient Authentication/Authorization);
* атаки на сессию;
* незащищенная передача данных в процессах аутентификации и авторизации;
* межсайтовое выполнение сценариев (Cross-Site Scripting);
* подделка HTTP-запросов (Cross-Site Request Forgery);
* смешивание параметров HTTP (HTTP Parameter Pollution);
* подмена контента (Content Spoofing);
* расщепление/сокрытие HTTP-запроса/HTTP-ответа (HTTP Request/Response Splitting/Smuggling);
* открытое перенаправление (Open Redirect);
* кликджекинг (Clickjacking);
* выполнение команд ОС (OS Commanding);
* внедрение операторов SQL (SQL Injection);
* внедрение операторов LDAP (LDAP Injection);
* внедрение серверных расширений (SSI Injection);
* внедрение операторов Xpath (Xpath Injection);
* внедрение операторов IMAP/SMTP (IMAP/SMTP Injection);
* переполнение буфера (Buffer Overflow);
* атака на функции форматирования строк (Format String Attack);
* доступность информации о каталогах, файлах и сценариях;
* предсказуемое расположение ресурсов (Predictable Resource Location);
* идентификация приложений (Web Server/Application Fingerprinting);
* чтение произвольных файлов;
* утечка информации (Information Leakage);
* стандартные сообщения об ошибках;
* обратный путь в каталогах (Path Traversal);
* раскрытие установочного пути (Full Path Disclosure);
* отказ в обслуживании (Denial of Service).

(Предлагаю таблицу ниже в точно таком же виде оставить в шаблоне, чтобы она не потерялась. Нужна или нет, решит менеджер и в случае необходимости сам впишет туда необходимые сведения.)

**Состав мероприятий**

Таблица ${номер} – Основные мероприятия

| **№** | **Состав мероприятий** | **Сроки проведения** | | **Потенциальные риски** |
| --- | --- | --- | --- | --- |
| **Начало** | **Окончание** |
|  | *Описание мероприятия* | *Дата* | *Дата* | *Описание возможных рисков* |
|  | *Описание мероприятия* | *Дата* | *Дата* | *Описание возможных рисков* |
|  | *Описание мероприятия* | *Дата* | *Дата* | *Описание возможных рисков* |
|  | *Описание мероприятия* | *Дата* | *Дата* | *Описание возможных рисков* |
|  | *Описание мероприятия* | *Дата* | *Дата* | *Описание возможных рисков* |

# **Подробное описание результатов и рекомендации по устранению всех выявленных недостатков**

## **${Наименование информационной системы/офиса/ЦОД 1}**

## **${Наименование объекта (url/имя сервера/наименование оборудования) и (или) IP-адрес объекта локальный/белый}**

#### ${Наименование уязвимости}

**Уязвимость**: ${Расположение уязвимости, описание уязвимости, ID уязвимости CVE, ID уязвимости CWE, скриншот уязвимости}

Успешная эксплуатация уязвимости злоумышленником может привести к следующим негативным последствиям: ${негативные последствия}

Причиной возникновения уязвимости является${причина возникновения уязвимости}.

**Порядок эксплуатации уязвимости**: ${Порядок эксплуатации уязвимости}

**Итоговый уровень риска**:

${критический, высокий, средний, низкий, информационный}.

CVSSv3.1: ${0-10}

(${метрики})

**Рекомендации**:

${рекомендации}

## **${Наименование информационной системы/офиса/ЦОД 2}**

## **${Наименование объекта (url/имя сервера/наименование оборудования) и (или) IP-адрес объекта локальный/белый}**

#### ${Наименование уязвимости}

**Уязвимость**: ${Расположение уязвимости, описание уязвимости, ID уязвимости CVE, ID уязвимости CWE, скриншот уязвимости, причина возникновения, возможные последствия}

Успешная эксплуатация уязвимости злоумышленником может привести к следующим негативным последствиям: ${негативные последствия}

Причиной возникновения уязвимости является${причина возникновения уязвимости}.

**Порядок эксплуатации уязвимости**: ${Порядок эксплуатации уязвимости}

**Итоговый уровень риска**:

${критический, высокий, средний, низкий, информационный}.

CVSSv3.1: ${0-10}

(${метрики})

**Рекомендации**:

${рекомендации}