Правила программы Bug Bounty

1. Область действия

Программа Bug Bounty **NOX** распространяется на все домены и сервисы, входящие в инфраструктуру проекта:
***.nox.info** и связанные домены.
Вознаграждения выплачиваются только за уязвимости, обнаруженные в сервисах основного скоупа. Остальные ресурсы могут быть рассмотрены с пониженным коэффициентом выплаты.

---

2. Исключения из программы

К рассмотрению принимаются только отчёты, содержащие **реальные проблемы безопасности**.
Не рассматриваются (невалидные отчёты):

- ошибки, не влияющие на безопасность (UI, орфография, UX);
- раскрытие общедоступной или публичной информации;
- фишинг, социальная инженерия, атаки с физическим доступом;
- утечки технических сведений (версии ПО, структура каталогов и пр.);
- необработанные отчёты сканеров или автоматизированных инструментов;
- clickjacking без влияния на безопасность;
- email spoofing без подтверждения эксплуатационного сценария.

---

3. Требования к отчётам

Отчёт должен содержать:

- подробное **описание уязвимости** и шаги воспроизведения;
- **анализ критичности** (влияние, потенциальные риски);
- **URL**, тип уязвимости, доказательства (скриншоты, видео).

Если отчёт не позволяет воспроизвести проблему или не содержит ключевых данных — вознаграждение не выплачивается.
При нарушении минимальных требований сумма вознаграждения может быть снижена.

---

4. Правила тестирования

- Используйте **только свои** аккаунты или те, чьи владельцы согласие.
- Запрещены любые действия, нарушающие **конфиденциальность, целостность или доступность** данных.
- Не допускаются атаки, способные причинить вред пользователям, сервисам или инфраструктуре (в т.ч. DDoS, социальная инженерия, физическое воздействие).
- Используйте **минимально необходимый PoC**. Если тест может повлиять на других пользователей, получите разрешение от администрации.
- Эксплуатация найденных уязвимостей после подтверждения их наличия — строго запрещена.

Несоблюдение этих правил может привести к **дисквалификации из программы**.

---

5. Правила выплат

- Вознаграждения выплачиваются **только за ранее неизвестные** и **подтверждённые** уязвимости.
- Дубликаты не оплачиваются: вознаграждение получает первый валидный отчёт, содержащий достаточные данные для воспроизведения.
- Размер вознаграждения определяется исходя из **критичности системы**, **рисков эксплуатации** и **уникальности находки**.

Уровень критичности	Основной скоуп
Критический	$5000
Высокий	$2000–$2500
Средний	$300–$1000
Низкий	$100

Администрация оставляет за собой право пересматривать размер вознаграждений в зависимости от особенностей инцидента.

---

6. Дублирующие отчёты

- Если аналогичная уязвимость уже была сообщена ранее, новый отчёт помечается как **дубликат**.

- Частичные совпадения (например, разные endpoints с одинаковым вектором атаки) могут быть объединены в одну категорию по решению команды безопасности.

---

7. Ответственность и соблюдение конфиденциальности

- Участники обязуются **не разглашать** сведения об уязвимостях до официального исправления.
- Запрещается публичное обсуждение, публикация PoC или деталей без разрешения администрации.
- За нарушение — аннулирование вознаграждения и возможное исключение из программы.

---

8. Каналы связи

Для отправки отчётов:
Техническая поддержка: support@nox.info (или же в личном кабинете при авторизации в сервисе).

---

9. Прочие условия

- Администрация может изменять правила программы без предварительного уведомления.
- Участие в программе означает **согласие со всеми условиями**.
- Программа не является конкурсом, лотереей или публичной офертой в юридическом смысле.