Политика информационной безопасности онлайн-магазина

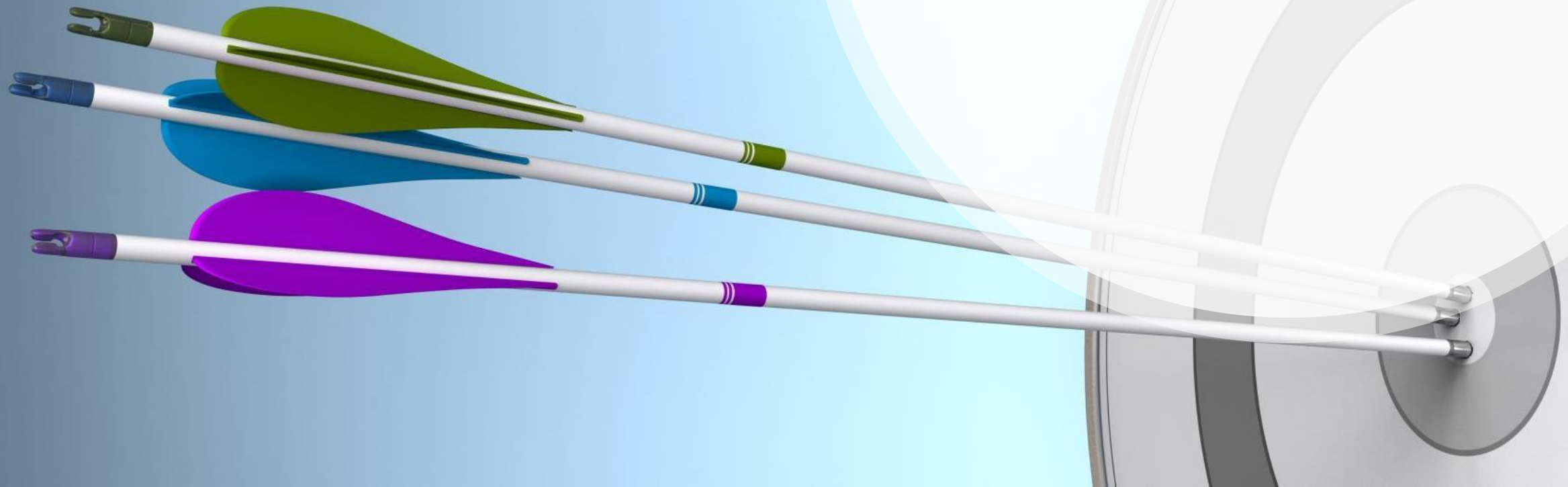
Мазенкова Ирина 4-1

Актуальность

- •В нынешнее время нередко люди совершают незаконную передачу или хранение личной и конфиденциальной информации: паролей, программных кодов и алгоритмов, авторских процессов и технологий.
- •В ноябре 2021 года кампания **StormWall** опубликовала результаты исследования, согласно которым интенсивность атак на коммерческие проекты выросла в 4 раза по сравнению с показателями прошлого года.
- •В большинстве случаев **главная цель** хакеров – украсть персональные данные пользователей.

Цель ПИБ

- **Главная цель** политики информационной безопасности – гарантия защиты данных от внешних и внутренних угроз.



Задачи ПИБ

Обеспечить данным:

•Конфиденциальность – доступ есть только у лиц, имеющих на это полномочия;

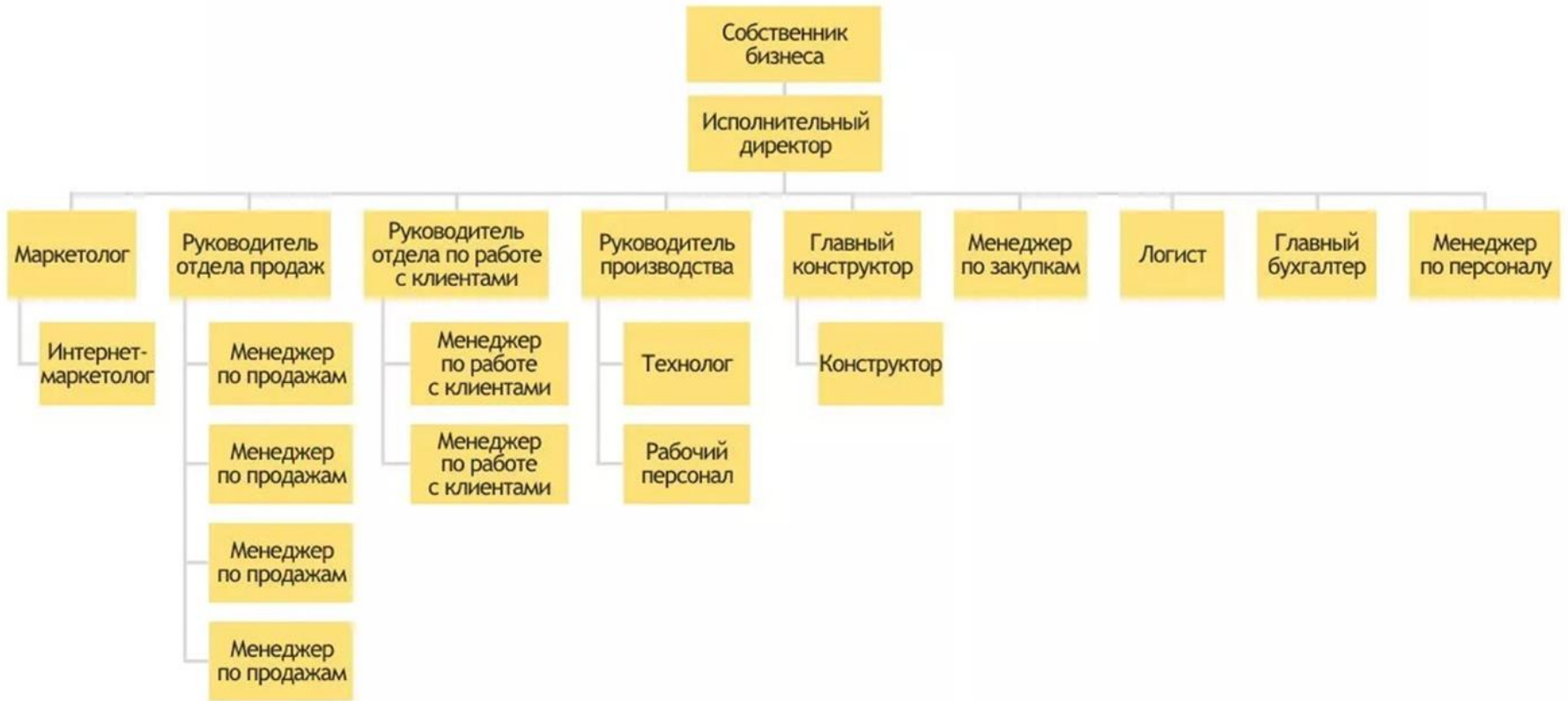
•Доступность информационных систем с находящимися в них данными конкретным сотрудникам, у которых есть право доступа к таким сведениям;

•Целостность – блокировка несанкционированного изменения информации;

•Подлинность – полнота и общая точность информации;

•Неотказуемость – возможность определить источник или авторство информации.

Организационная структура



Объекты защиты (работают с информацией)

- КОМПЬЮТЕРЫ И СЕТИ;

- ОС, СЕРВЕРА И СУБД;

- САЙТ ИНТЕРНЕТ-МАГАЗИНА.

Субъекты (инициирует поток информации)

- сотрудники и пользователи (их персональные данные);

- рабочие станции, используемые в работе.

Основные **угрозы**

- утечка данных пользователей и сотрудников;
- заражение программного кода (снижение работоспособности сайта и его рейтинга в поисковых системах);
- атаки, направленные на отказ в обслуживании (DDOS атаки);
- воровство трафика (злоумышленное перенаправление пользователей на сторонние или поддельные фишинговые сайты);
- уничтожение или разрушение средств обработки информации и связи.

Оценка **угроз**

ОПИСАНИЕ АТАКИ	УЩЕРБ	ВЕРОЯТНОСТЬ	РИСК
Взлом базы данных	4	0,1	0,4
Отказ аппаратуры	1	0,1	0,1
Воровство трафика	2	0,2	0,4
Утечка персональных данных	4	0,1	0,4
DDoS-атака	2	0,3	0,6
Ошибка ПО	1	0,3	0,3
Итого	14	1,1	2,2

Меры **защиты**

1.Соблюдайте личную безопасность.

•Используйте генератор паролей.

•Один пароль для одной системы.

• Для хранения паролей в браузере установите специальное расширение.

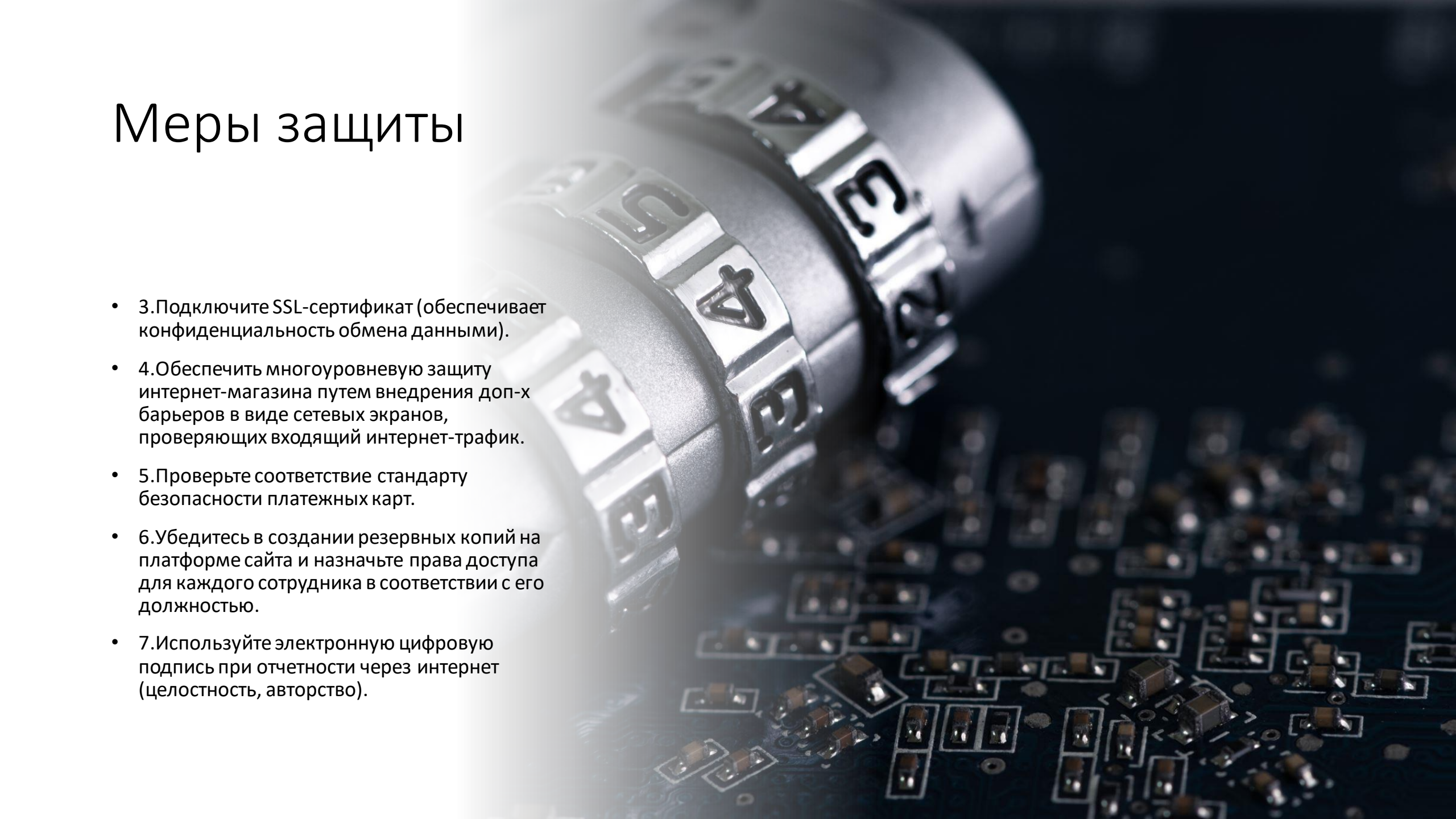
2.Используйте надежный хостинг для сайта.

•Степень защиты дата-центра (место, в котором находятся физические накопители хостинга) – Tier III.

•Создание бэкапов по возможности на удаленный сервер.

•Подключение защиты от DDoS-атак и антивируса (регулярно обновлять их модули и базы).

Меры защиты



- 3.Подключите SSL-сертификат (обеспечивает конфиденциальность обмена данными).
- 4.Обеспечить многоуровневую защиту интернет-магазина путем внедрения доп-х барьеров в виде сетевых экранов, проверяющих входящий интернет-трафик.
- 5.Проверьте соответствие стандарту безопасности платежных карт.
- 6.Убедитесь в создании резервных копий на платформе сайта и назначьте права доступа для каждого сотрудника в соответствии с его должностью.
- 7.Используйте электронную цифровую подпись при отчетности через интернет (целостность, авторство).

Спасибо за внимание!