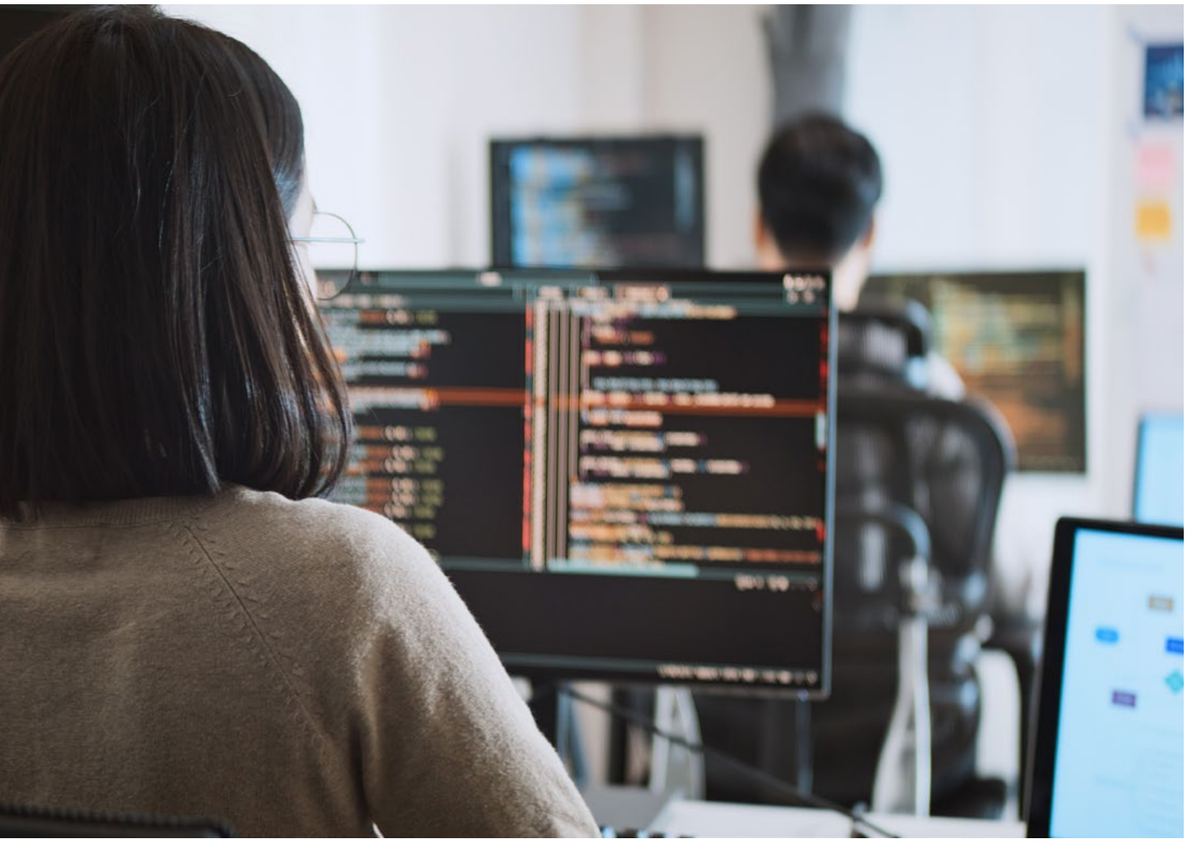
# Информационная безопасность и защита персональных данных

Тренд на цифровизацию розничной торговли усиливает актуальность темы информационной безопасности и защиты персональных данных. Обработка персональных данных клиентов и сотрудников является неотъемлемой частью операционной деятельности Группы «Магнит». В связи с этим построение надежной системы информационной безопасности и обеспечение конфиденциальности персональных данных являются приоритетом для Компании. Для обеспечения устойчивости ключевых бизнес-систем, непрерывности работы сервисов Компании и защиты персональных данных пользователей «Магнит» на постоянной основе совершенствует систему информационной безопасности. Так, в отчетном периоде «Магнит» провел внутреннюю оценку зрелости системы управления информационной безопасностью, по результатам которой были выделены приоритетные направления для развития и сформированы конкретные планы мероприятий на следующий год.

В 2025 г. ввиду растущих внешних киберугроз в Компании была сформирована программа непрерывности бизнеса на среднесрочную перспективу. Она включает в себя ряд ключевых мероприятий, направленных на повышение устойчивости системы информационной безопасности Компании к внешним атакам.

Для обеспечения контроля системы информационной безопасности Компания регулярно осуществляет комплексное сканирование внешнего и внутреннего периметров. Оценка рисков кибербезопасности также проводится на регулярной основе.



**Ключевые направления обеспечения информационной безопасности**

### Развитие систем защиты информации

- Регулярная оценка уровня соответствия систем информационной безопасности внутренним стандартам и законодательству
- Поддержка и развитие физической и облачной ИТ-инфраструктуры, инвестиции в ЦОД

### Обучение сотрудников в области кибербезопасности

- Обязательные курсы по работе с персональными данными и информационной безопасности для всех сотрудников
- Профильное обучение сотрудников, ответственных за обеспечение информационной безопасности Компании

### Программа для поиска уязвимостей Bug Bounty

В 2025 г. после успешного завершения закрытого этапа «Магнит» сделал публичной программу Bug Bounty с целью усиления защищенности своих цифровых сервисов. Данная инициатива привлекает глобальное сообщество белых хакеров[1] к поиску сложных уязвимостей и логических ошибок, которые могут остаться незамеченными при автоматизированном сканировании ИТ-систем.

В рамках программы тестированию подвергаются ключевые клиентские и сервисные ресурсы розничной сети, включая мобильное приложение, сайт доставки, портал программы лояльности и другие цифровые сервисы.

Для повышения мотивации участников в рамках программы действует дифференцированная система вознаграждений, размер которых зависит от критичности выявленной уязвимости.

Подробнее с условиями программы можно ознакомиться на сайте.

Обработка персональных данных в Компании осуществляется в строгом соответствии с требованиями Федерального закона № 152 «О персональных данных» от 27.07.2006 N 152-ФЗ и других нормативных актов.

Обеспечение конфиденциальности данных в Группе «Магнит» реализуется по двум ключевым направлениям: соответствие техническим и методологическим требованиям регуляторов и обучение сотрудников в области информационной безопасности и работы с персональными данными.

Для сотрудников «Магнита» действует специализированная служба поддержки по вопросам работы с персональными данными. Любой сотрудник может направить обращение специалистам Департамента информационной безопасности для получения консультации или проведения правовой экспертизы документов и проектов, затрагивающих процессы обработки персональных данных. Кроме того, через данный канал можно сообщить о подозрении или выявленном факте неправомерной передачи либо утечки персональных данных.

В результате эффективной работы системы информационной безопасности в 2025 г. случаев утечки персональных данных клиентов и сотрудников «Магнита» зафиксировано не было.

1 Белый хакер – специалист по информационной безопасности, который легально исследует ИТ-системы на уязвимости с целью выявить и устранить бреши до того, как их смогут использовать злоумышленники.