Информационная безопасность

В современном мире информация – важный ресурс, сохранение которого имеет большое значение для деятельности предприятий. Мы стремимся соответствовать лучшим стандартам в этой области и успешно предотвращаем кибератаки и другие ИТ-инциденты.

Ключевые документы

Внутренние документы Компании:

- Политика информационной безопасности
- Политика контроля систем управления информационной безопасностью (СУИБ)
- Парольная политика
- Положение по управлению учетными данными и доступами пользователей
- Порядок создания и внесения изменений в правила межсетевых экранов
- Стандарт соблюдения требований информационной безопасности к созданию информационных систем и сервисов
- Политика обработки персональных данных

Нормативные акты:

- Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
- Постановление Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении Типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и Типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»
- Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ
- Федеральный закон «Об информации, информационных технологиях и о защите информации»
- Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

Приоритетные ЦУР ООН

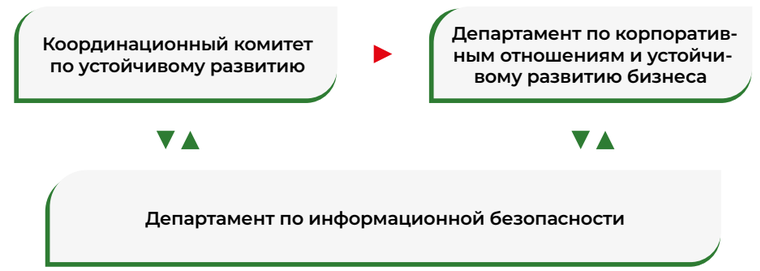
16 МИР, ПРАВОСУДИЕ И ЭФФЕКТИВНЫЕ ИНСТИТУТЫ

Наш подход к управлению информационной безопасностью

Защита интересов «Магнита» в информационной сфере основана на комплексе взаимосвязанных организационно-технических мероприятий, образующих единую систему управления и обеспечения информационной безопасности. Комплексный подход позволяет нам обеспечить защиту от современных киберугроз, соответствовать законодательным требованиям Российской Федерации и международным стандартам, а также предотвратить причинение финансового, репутационного и другого ущерба. Система защиты информации «Магнита» построена и развивается с учетом лучших мировых практик.

В нашей Компании существует процесс внутреннего ИТ-аудита, для чего мы создали отдельное подразделение. Мы регулярно проводим оценку рисков по направлению информационной безопасности и ежеквартально тестируем наши ИТ-системы.

Система управления информационной безопасностью



- Административное подчинение.
- Координация в рамках реализации Стратегии по устойчивому развитию, консультационная поддержка.

Информационная безопасность (продолжение)

Система защиты от кибератак

Мы взяли на себя обязательства по организации системы по защите от кибератак, для выполнения которых применяем решения по выявлению и устранению уязвимостей на информационных устройствах, выявлению вирусной активности и 0-day[1] атак, отслеживаем и реагируем на инциденты безопасности. Все внешние ИТ-сервисы «Магнита» проходят архитектурный контроль. Мы проводим плановое обновление сетевых устройств, серверов и программного обеспечения.

Мы ежедневно сканируем все внешние адреса Компании на наличие известных уязвимостей и устраняем возникшие угрозы. Все веб-сервисы «Магнита» защищаются через средства WAF, или файрволлы, предназначенные для обнаружения и блокирования сетевых атак на веб-приложения. Мы активно используем решения Анти-ДДОС[2] и постоянно сканируем открытые порты из интернета. Дважды в год «Магнит» инициирует внешние независимые тестирования на проникновение в систему Компании.

В 2022 г. мы наблюдали значительный рост числа кибератак на ИТ-активы «Магнита». Зафиксированы десятки тысяч сканирований и сетевых атак злоумышленников, а также более 500 тыс. попыток заражения ИТ-инфраструктуры вредоносным программным обеспечением через почтовую систему. Мы приняли дополнительные меры для повышения уровня защищенности, что позволило нам успешно отразить кибератаки и избежать сбоев в работе инфраструктуры.

Кроме того, мы начали переход на отечественные решения для обеспечения информационной безопасности, так как иностранные вендоры, поставляющие подобные системы, покинули рынок России. В 2023 г. мы продолжим внедрять средства информационной защиты, предлагаемые ведущими российскими разработчиками.

Чтобы гарантировать информационную безопасность наших покупателей, мы внедрили систему «Антифрод», которая предусматривает:

- защиту от перехвата и кражи аккаунтов мобильного приложения «Магнит»;
- защиту от начисления и списания мошенниками баллов программы Лояльности;
- контроль доступа к данным карт лояльности для предотвращения утечки информации о балансе и номерах карт покупателей.

В 2023 г. мы планируем провести аудит процессов обработки персональных данных на соответствие требованиям Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ. В дополнение к этому мы намерены развивать процессы DevSecOps[3] и стандартизировать подходы и инструменты в командах разработки.

Обучение сотрудников безопасному использованию ИТ-систем

Один из приоритетов нашей политики информационной безопасности – повышение осведомленности сотрудников о правилах киберзащиты. Мы уделяем особое внимание обучению и профессиональному развитию сотрудников ИТ-дирекции, которые участвуют в процессе обеспечения работоспособности ИТ-инфраструктуры и информационных систем «Магнита». Сотрудники других подразделений, которые пользуются ИТ-системами в своей ежедневной работе, также проходят регулярные тренинги. Мы проводим регулярный инструктаж сотрудников различных департаментов, ответственных за организацию обработки персональных данных.

Направления повышения осведомленности сотрудников по информационной безопасности

- **Безопасная работа с информационными системами**
- **Парольная политика Компании**
- **Выявление фишинга и атак типа социальной инженерии**
- **Стандарты информационной безопасности Компании**

Чтобы обеспечить безопасность удаленной и гибридной работы, мы разработали и запустили распределенную, географически отказоустойчивую и масштабируемую система удаленного доступа для всех сотрудников головного офиса и филиалов. Это позволило нам обеспечить непрерывность бизнес-процессов и увеличить мобильность сотрудников. Мы рассматриваем возможности для оптимизации офисного пространства, расширяем географию возможных кандидатов на должности в Компании, а работа наших сотрудников становится комфортнее.

Мы продолжаем работать над вопросами информационной безопасности в контексте перехода на удаленный формат. В частности, теперь наши сотрудники обязательно используют второй фактор при аутентификации в момент подключения, а также применяют различные продукты и политики безопасности на корпоративных устройствах, которые отслеживают и блокируют попытки компрометации и несанкционированного доступа.

Безопасность персональных данных

Мы разработали системный подход к защите персональных данных наших заинтересованных сторон. «Магнит» ведет постоянный контроль за имеющимися и планируемыми к внедрению информационными системами на предмет корректной и правомерной обработки персональных данных. Персонал ИТ-дирекции и сотрудники, работающие с данными пользователей, проходят обучение, а ответственные за организацию обработки персональных данных проходят регулярные инструктажи. Мы разработали формы согласия на обработку персональных данных, которые заполняются каждым сотрудником, а также назначили ответственных за организацию и контроль процесса защиты данных.

Для нас важно повысить осведомленность всех сотрудников Компании в вопросах информационной безопасности в целом и в вопросах защиты персональных данных в частности. Мы сопровождаем и контролируем бизнес-процессы, в рамках которых ведется обработка персональных данных, для предотвращения рисков получения санкций от государственных органов. Мы также консультируем специалистов дочерних компаний по вопросам, связанным с регламентацией обработки персональных данных.

В «Магните» налажен механизм подачи заявлений о нарушении работы с персональными данными. В нашей Компании ведется журнал регистрации ИТ-инцидентов в информационных системах, обрабатывающих персональные данные, а также журнал запросов и обращений внешних стейкхолдеров по вопросам персональных данных.

Мы регулярно проводим оценку рисков в рамках внутреннего аудита, а также анализируем обрабатываемые данные, разрабатываем и актуализируем модели угроз для информационных систем, формируем и внедряем технические решения для устранения таких угроз, разрабатываем инструкции и регламенты, направленные на приведение к соответствию требованиям законодательства в области персональных данных.

[1] 0-day, или уязвимость нулевого дня — неустраненные уязвимости, а также вредоносные программы, против которых еще не разработаны защитные механизмы.
[2] Anti-DDoS – система защиты от DDoS-атак, нацеленных на выведение из строя вычислительной системы путем постоянного потока запросов.
[3] Практика интеграции тестирования безопасности в каждый этап процесса разработки программного обеспечения (англ. Development Security Operations).