ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ: РОЛЬ И ОТВЕТСТВЕННОСТЬ ФОНДА

Информационная безопасность является неотъемлемой частью стабильной работы информационной сети, защиты национальных интересов и поддержания доверия со стороны общества и партнёров. С развитием цифровых технологий АО «Самрук-Қазына» и группа компаний Фонда, постоянно повышает уровень информационной безопасности, для предотвращения киберугроз, а также приводит требования в области информационной безопасности в соответствие с законодательными нормами.

Ключевыми стратегическими целями Фонда в данной области являются — обеспечение доступности, целостности, конфиденциальности и отказоустойчивости.

СОЗДАНИЕ КУЛЬТУРЫ БЕЗОПАСНОСТИ

В рамках укрепления информационной безопасности Фонд приступил к внедрению международного стандарта ISO 27001. Согласно приказу Председателя Правления Фонда, организована рабочая группа для создания реестра информационных активов и их классификации по уровням значимости.

Данная классификация предусматривает разделение на следующие категории:

Информация:

- Особый информационный актив;
- Стратегический информационный актив;
- Защищаемый информационный актив;
- Базовый информационный актив.

Кадры. Введена иерархия доступа, определяющая различные уровни доступа для работников в зависимости от их роли и ответственности.

Физическая инфраструктура. Проведены работы по защите информации на физическом и логическом уровнях в ИТ-инфраструктуре.

Обучение. Для развития навыков кибергигиены среди работников Фонда проводятся обучающие сессии и тестирования с использованием специализированного программного обеспечения.

СОЗДАНИЕ ЭФФЕКТИВНЫХ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В Фонде внедрены «Основные правила политики информационной безопасности» с приложениями в виде методик, руководств и правил, которые регламентируют деятельность специалистов в области информационной безопасности (ИБ) и информационных технологий (ИТ), а также всех работников в части исполнения мер обеспечения информационной безопасности.

Проводятся работы по разработке Корпоративного стандарта информационной безопасности, регулирующего общий свод правил обеспечения информационной безопасности и управлению процессом координации деятельности в группе компаний Фонда.

ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

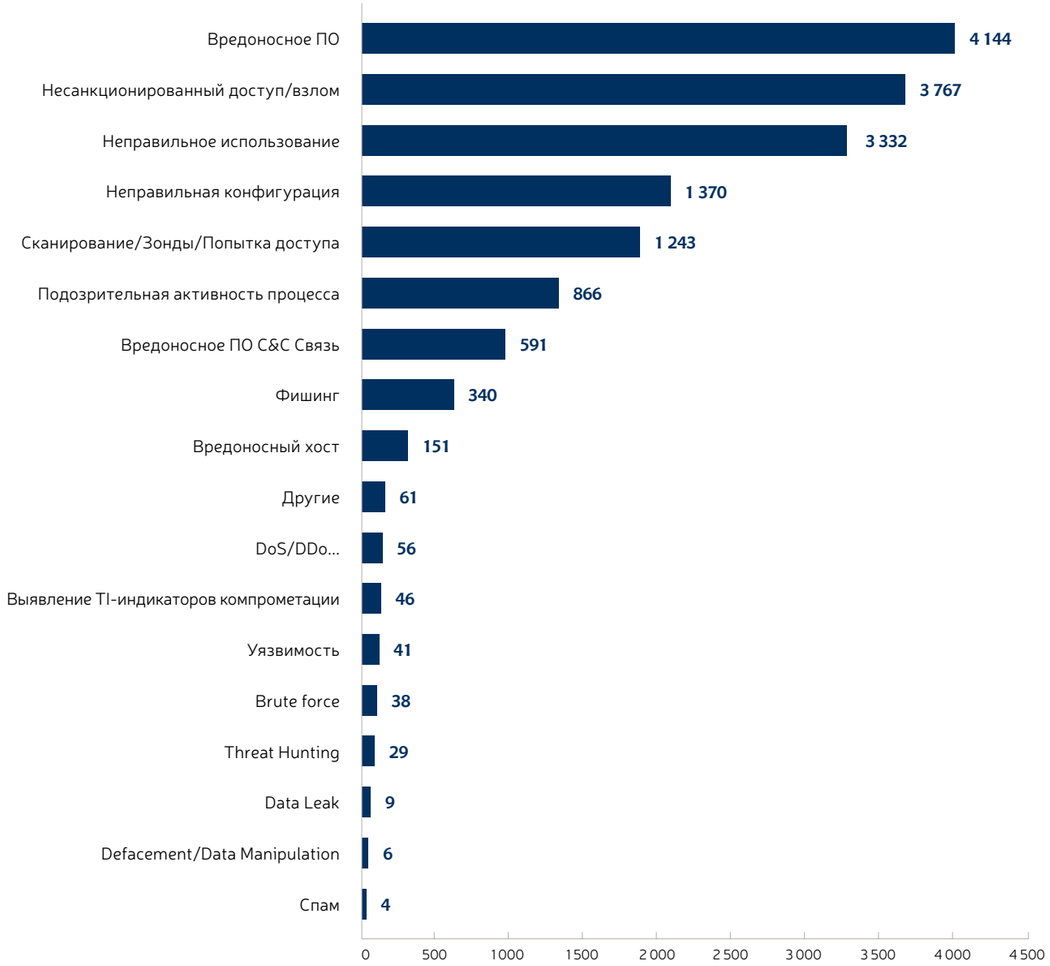
- Проведены технические работы по приведению в соответствие ИТ-инфраструктуры.
- Проведена оптимизация используемых продуктов по информационной безопасности, внедрены современные программные продукты для мониторинга, предотвращения утечки информации, сканирования и получения оперативных сведений об уязвимостях.

ПРОТИВОСТОЯНИЕ КИБЕРАТАКАМ

- В условиях Фонда для сопровождения систем информационной безопасности и оперативного реагирования на внешние и внутренние угрозы IT-инфраструктуры создан мониторинговый центр.
- Проведен аудит (пентест) внешней инфраструктуры. Выявленные уязвимости своевременно устранены техническими специалистами Фонда.

В 2023 году проведены аудиты портфельных компаний Фонда на предмет соответствия требованиям информационной безопасности, по результатам которых разработаны рекомендации по повышению уровня информационной безопасности. Ежегодно формируется регистр рисков по кибербезопасности, а также ежеквартальные отчеты по рискам, в том числе касающиеся компаний группы Фонда.

СТАТИСТИКА ИНЦИДЕНТОВ В РАЗРЕЗЕ ТИПОВ УГРОЗ ЗА 2023 ГОД В ГРУППЕ ФОНДА



СТАТИСТИКА ИНЦИДЕНТОВ ЗА 2023 ГОД ПО ГРУППЕ ФОНДА