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» 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 устойчивости.

СОЗДАНИЕ КУЛЬТУРЫ БЕЗОПАСНОСТИ

В рамках укрепления информационной безопасности в соответствии с требованиями международного стандарта ISO 27001 проведены работы по анализу и оптимизации IT-инфраструктуры.

Согласно проведённой оценке зрелости процессов информационной безопасности, в которой были оценены 11 доменов по CobiT 4.1 DS5 (Deliver and Support), система управления информационной безопасностью соответствует «определённому уровню» зрелости.

В Фонде внедряются лучшие практики, определены процессы, политики, процедуры, документированы основные действия в области информационной безопасности. Ответственность и подотчётность определены, назначены владельцы процессов. Имеется формализованное и структурированное информирование руководства Фонда.

Физическая инфраструктура.
В ходе комплексного обследования были выявлены существующие проблемы, потенциальные точки отказа и уязвимости IT-инфраструктуры.

Подготовлена подробная документация по внесенным изменениям и разработаны рекомендации для плавного перехода на обновленную конфигурацию с минимальными рисками и перебоями в работе.

В результате проделанной работы удалось значительно повысить надежность, безопасность и эффективность IT-инфраструктуры, что обеспечит её стабильное функционирование и соответствие современным требованиям.

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

СОЗДАНИЕ ЭФФЕКТИВНЫХ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В группе компаний Фонда внедрен «Корпоративный стандарт информационной безопасности» регулирующий общий свод правил обеспечения информационной безопасности и управления процессом координации деятельности. В Фонде проведены работы по внедрению требований «Основных правил информационной безопасности» и соответствующих правил и регламентов.

В рамках эффективного управления процессом категоризации информационных активов Фонда, установления требований по обеспечению информационной безопасности для защищаемых информационных активов, а также назначения уровней доступа сотрудникам инициирована разработка «Методика классификации информационных активов в АО «Самрук-Қазына». Планируется внедрение процесса установления градаций важности информации и отнесение конкретных информационных ресурсов к соответствующим категориям по степени их конфиденциальности.

ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Проведена оптимизация размещения серверного и сетевого оборудования для повышения производительности и удобства обслуживания.

Внедрены современные программные продукты для мониторинга, предотвращения утечки информации, сканирования и получения оперативных сведений об уязвимостях.

ПРОТИВОСТОЯНИЕ КИБЕРАТАКАМ

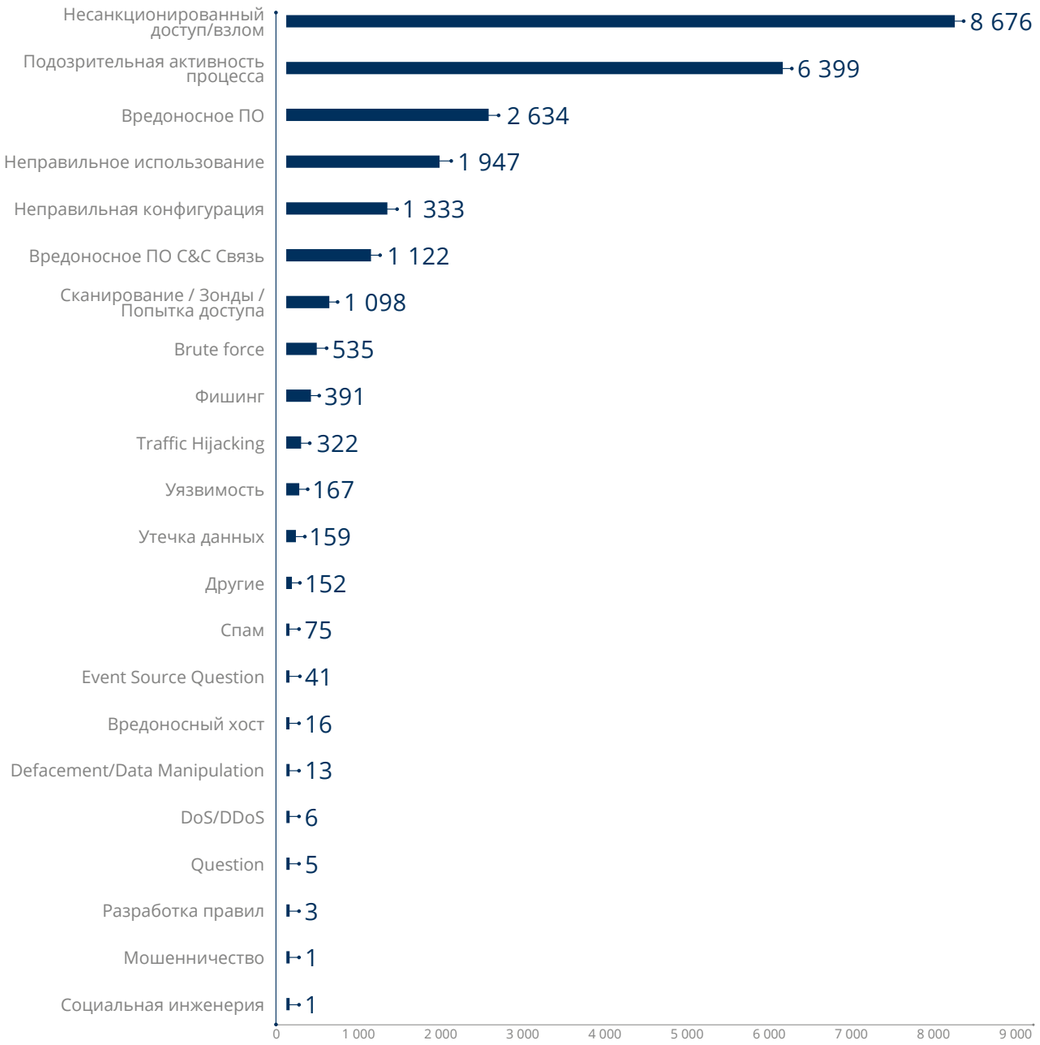
В условиях Фонда для сопровождения систем информационной безопасности и оперативного реагирования на внешние и внутренние угрозы IT-инфраструктуры работает мониторинговый центр.

Согласно требованиям внутренних документов Фонда и применимых стандартов в области информационной безопасности, производилось сканирование с использованием специализированного ПО не менее 6 раз за отчетный период.

В 2024 году проведены аудиты портфельных компаний Фонда на предмет соответствия требованиям информационной безопасности, по результатам которых разработаны рекомендации по повышению уровня информационной безопасности.

Для идентификации рисков по кибербезопасности составляется перечень источников риска и событий, который позволяет оценить негативные воздействия на деятельность Фонда. Также формируются ежеквартальные отчеты по рискам.

СТАТИСТИКА ИНЦИДЕНТОВ В РАЗРЕЗЕ ТИПОВ УГРОЗ ЗА 2024 ГОД В ГРУППЕ ФОНДА



СТАТИСТИКА ИНЦИДЕНТОВ ЗА 2024 ГОД ПО ГРУППЕ ФОНДА