Информационная безопасность

Для обеспечения бесперебойной работы объектов критической информационной инфраструктуры завершен первый этап создания комплексной системы информационной безопасности (КСИБ). В ходе реализации проекта в филиалах Компании внедрены три подсистемы информационной безопасности:

- подсистема контроля действий привилегированных пользователей;
- подсистема анализа защищенности;
- подсистема сбора, анализа и корреляции событий информационной безопасности.

Создание комплексной многоуровневой системы информационной безопасности позволит обеспечить устойчивую работу объектов критической информационной инфраструктуры филиалов Компании в условиях проведения целевых кибератак.

Результаты в данной области по итогам 2021–2023 годов

Направления инновационного развития	2021	2022	2023
Количество событий информационной безопасности (обработано 100 %), шт.	4 680	2 087	1 220
Количество атак, шт.	185 385	5 438 098	60 213
Из них отражено, %	*100*	*100*	*100*
Количество утечек данных, шт.	0	0	0
Из них утечек персональных данных клиентов, %	*0*	*0*	*0*

GRI 418-1

Фактов утечки персональных данных работников Компании или клиентов, а также жалоб на такие утечки, полученных от третьих лиц, регуляторов в области обеспечения безопасности информации, не было.

Планы по развитию направления

В 2024 году мы планируем провести пересмотр результатов категорирования объектов критической информационной инфраструктуры 2019 года[1]. Сведения о результатах пересмотра категории значимости будут направлены в федеральный орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

В 2024–2026 годах запланирована дальнейшая реализация мероприятий по созданию КСИБ по программе «Информационная безопасность «Россети Центр».

В 2024 году в рамках второго этапа инвестиционной программы предусмотрено внедрение двух подсистем информационной безопасности:

- антивирусной защиты технологического сегмента филиалов;
- анализа и противодействия целевым компьютерным атакам.

Выполнение мероприятий второго этапа позволит обеспечить устойчивое функционирование категорированных объектов критической информационной инфраструктуры в условиях целевых компьютерных атак.

[1] В соответствии с пунктом 21 Постановления Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», положениями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Импортозамещение и взаимодействие с производителями оборудования

В 2023 году мы проанализировали возможность замещения импортной продукции, выявленной в составе проектов инвестиционной программы, и сформировали перечень импортной продукции, в том числе радиоэлектронной, которую планируется приобретать для инвестиционных проектов на период 2023–2027 годов[1].

Кроме того, разработан план перехода Компании на преимущественное использование российской радиоэлектронной продукции до 2024 года.

Ведется учет в типовых договорах под ключ и проектирование требований по минимизации применения импортного оборудования.

Подготовлен отчет по целевым показателям доли закупки продукции в закупках оборудования, сформированы сведения о закупленной импортной и отечественной продукции, в том числе у предприятий оборонно-промышленного комплекса.

Доля импортного оборудования и материалов в общем объеме закупок оборудования, %

Доля импорта в закупках программного обеспечения, %

Компания стремится выполнять задачи по импортозамещению, постепенно снижая долю закупленных импортных материалов и оборудования. В 2023 году доля закупок импортных материалов ниже планового показателя на 4,3 п. п., а доля закупок импортного программного обеспечения ниже планового значения на 20 п. п.

КПЭ по радиоэлектронной продукции

Наименование КПЭ	2023 год (факт)
Доля расходов на закупку российской радиоэлектронной продукции в общем объеме расходов на закупку радиоэлектронной продукции, %	86
Увеличение вложений в российскую радиоэлектронную продукцию, млн руб.	53,93

Мы также тестировали отечественное серверное оборудование и программное обеспечение[2]. Разработаны программа и методика испытаний оборудования производства «Аквариус» и Kraftway. Проведено тестирование отечественного ПО компаний Alt Linux, Astra Linux, Tantor, VK Teams и др.

Для налаживания взаимодействия с отечественными и иностранными производителями оборудования и радиоэлектронной продукции, а также следуя требованиям Правительства Российской Федерации[3], мы направили в 80 российских компаний по производству радиоэлектронной продукции запросы[4] о наличии оборудования их производства в Реестре российской радиоэлектронной промышленности (РЭП) или о планируемых сроках внесения продукции в Реестр, чтобы у нас была возможность использовать такое оборудование на своих объектах.

Сформирована прогнозная потребность в импортном оборудовании, в том числе радиоэлектронном, на 2024 год.

Мы планируем проводить ежеквартальный сбор отчетной информации по закупкам, чтобы контролировать корректность данных о производителе и стране происхождения приобретенного оборудования и материалов.

[1] Письмо от 10.04.2023 № ТЕ/ЦА-МР1/926.
[2] В рамках приказа «Россети Центр» от 27.11.2023 № 431-ЦА.
[3] Постановление Правительства Российской Федерации от 10.07.2019 № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
[4] Письмо от 13.07.2023 № МР1-ЦА/57/1014 «О включении оборудования в реестр РЭП Минпромторга России».