БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

МИРОВЫЕ ТЕНДЕНЦИИ УГРОЗ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Подразделения информационной безопасности ПАО «МТС» в 2019 году успешно реализовали комплекс организационно-технических мероприятий, который позволил обеспечить соответствие систем управления и обеспечения информационной безопасности законодательным требованиям Российской Федерации, требованиям международных стандартов, современному уровню киберугроз и предотвратить причинение Группе МТС финансового, репутационного и иного ущерба.

Наибольший интерес для злоумышленников в 2019 году представляли: информационные активы (массивы) с персональными данными и телеметрией потребителей услуг связи, данные финансовых транзакций, ноу-хау в области методов обработки больших данных и искусственного интеллекта, информация ограниченного доступа.

По оценке экспертов Компании, вектор атак 2019 года сохранится в ближайшей перспективе и будет направлен на корпоративные информационные системы управления, обработки и хранения информации. Основные направления роста кибернапряженности для корпоративного сектора:

- развитие методов и форм целенаправленных атак (Advanced Persistent Threat) на основе технологий искусственного интеллекта и глубинного обучения;
- социальная инженерия и прямая вербовка персонала компаний;
- атаки на корпоративный сегмент с использованием оконечного пользовательского оборудования, связанного в управляемые интеллектуальные бот-сети;
- недостаточная защищенность и уязвимость облачных сервисов и решений для реализации защищенного интернета вещей (IoT) отечественного производства;
- наличие уязвимостей в программном коде коммерческих и собственных ИТ-решений;
- использование личного мобильного оборудования работников, не имеющего достаточных средств защиты информации, для доступа к информации ограниченного доступа;
- удаленная работа сотрудников, повышающая риск несанкционированного доступа к корпоративным объектам защиты.

В законодательной сфере следует ожидать сохранения тенденции распространения обязательных мер защиты информации на негосударственные информационные ресурсы (персональные данные, профессиональную и коммерческую тайну, сеть связи общего пользования, объекты критической информационной инфраструктуры и др.).

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Риск	Описание / факторы риска
Риск нарушения безопасности информации	Нарушение конфиденциальности, целостности или доступности информации из-за несоответствия корпоративной системы защиты информации актуальным угрозам безопасности информации, невыполнения администраторами и пользователями информационных систем или партнерами ПАО «МТС» установленной политики информационной безопасности компании. Как следствие, возможный ущерб из-за утечек сведений, составляющих коммерческую тайну, претензий физических лиц или партнеров из-за нарушения безопасности персональных данных, тайны связи, коммерческой тайны партнеров или иной информации ограниченного доступа
Регуляторные риски информационной безопасности	Санкции контролирующих органов или отрицательные заключения аудиторов (прокуратура, Минкомсвязи России, Роскомнадзор, ФСТЭК и ФСБ России, контролирующие органы стран присутствия, аудиторы SOX, PCI DSS и др.) из-за невыполнения требований российского, международного или национальных законодательств в странах присутствия по обеспечению безопасности информации, охраняемой законами. Кроме того, законы устанавливают к одному объекту правого регулирования разные требования по ИБ, которые могут не совпадать. При этом приоритет законов не установлен
Контрактные риски информационной безопасности	Отказ в заключении государственных или иных контрактов из-за несоответствия конкурсным условиям по информационной безопасности (отсутствие лицензий ФСТЭК и ФСБ России, российских или международных сертификатов на процессы и системы ИБ, необходимой инфраструктуры ИБ для предоставления услуг и др.)

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В МТС

- Система защиты информации в МТС представляет собой единый комплекс взаимоувязанных организационно-технических мероприятий с централизованной инфраструктурой и унифицированными по компаниям Группы МТС процессами управления и обеспечения информационной безопасности. Система построена с учетом лучших мировых практик на основе международных стандартов серии ISO 27000 и 15408.
- Система защиты персональных данных обеспечивает третий уровень защищенности ПД в соответствии с требованиями законодательства Российской Федерации.
- Защита тайны связи в сетях связи с встроенными в средства связи механизмами защиты информации соответствует международным стандартам связи и требованиям отраслевого регулятора.
- ПАО «МТС» является лицензиатом ФСТЭК и ФСБ России на деятельность по технической и криптографической защите конфиденциальной информации и мониторингу событий ИБ и может оказывать соответствующие услуги.

РЕЗУЛЬТАТЫ И ДОСТИЖЕНИЯ 2019 ГОДА

- Британский институт стандартов (British Standards Institution) впервые сертифицировал корпоративную Систему менеджмента информационной безопасности ПАО «МТС» на соответствие международному стандарту ISO/IEC27001:2013 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS и выдал сертификат № ISO 719403. Это также расширяет возможности участия компании в конкурсах и тендерах, ориентированных на международные стандарты ИБ.
- Силами подразделений безопасности в 2019 году предотвращено причинение бизнесу ущерба (финансового, репутационного или иного) в результате кибератак на компанию.
- Обеспечена непрерывность всех бизнес- и технологических процессов в соответствии с требованиями регуляторов, акционеров и руководства ПАО «МТС».
- Увеличено количество клиентов коммерческой услуги по мониторингу и реагированию на инциденты ИБ.
- В целях выполнения требований Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в 2019 году проведены следующие мероприятия:

  - создана комиссия по категорированию объектов критической информационной инфраструктуры (КИИ) ПАО «МТС»;
  - проведено категорирование объектов КИИ ПАО «МТС» в соответствии с методикой постановления Правительства Российской Федерации № 127;
  - утвержден и направлен в ФСТЭК России перечень объектов КИИ ПАО «МТС»;
  - разработан технический проект на создание системы безопасности объектов КИИ ПАО «МТС».
- Обеспечена поддержка новой структуры управления Компании посредством унификации процесса формирования требований информационной безопасности, организован учет объектов защиты и их характеристик.
- В целях обеспечения безотказной работы специальных комплексов, установленных на сети ПАО «МТС», организованы и на постоянной основе проводятся мероприятия по профилактике и технической поддержке оборудования и ПО.
- В рамках выполнения задач по реализации требований Федерального закона № 374-ФЗ на сети ПАО «МТС» ведутся работы по внедрению специальных комплексов в соответствии с согласованной с ФСБ России концепцией и сроками реализации Закона.
- На сетях связи установлены специальные комплексы, наличие которых обеспечивает возможность предоставления новых услуг и сервисов: NB-IoT, MTC Connect, WiFi Calling, VoLTE/ViLTE, WiFi для бизнеса, Виртуальная АТС.
- Работа по модернизации специальных комплексов, обеспечивающих деятельность уполномоченных государственных органов, проводилась на плановой основе, в соответствии с утвержденной инвестиционной программой, в строгом соответствии с требованиями НПА. Запланированные мероприятия выполнены в полном объеме.

ОСНОВНЫЕ ЗАДАЧИ В ОБЛАСТИ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА 2020 ГОД

- Обеспечение соответствия Системы менеджмента информационной безопасности ПАО «МТС» международному стандарту ISO/IEC27001:2013.
- Совершенствование мер и средств защиты информации одновременно с процессом внедрения новых информационных технологий.
- Контроль за соблюдением требований по сертификации оборудования и ПО информационной защиты под стандарты ФСТЭК и организация сертификации по требованиям ФСТЭК и ФСБ России новейших средств защиты информации при обеспечении защиты персональных данных.
- Реализация мер защиты, установленных нормативными правовыми актами Минкомсвязи России, ФСТЭК и ФСБ России, которые обеспечивают минимально достаточный уровень безопасности информации.
- Участие в работе регуляторов, общественных организаций, НП «Цифровая экономика» по совершенствованию законодательства по ИБ.
- Создание системы безопасности объектов КИИ ПАО «МТС».

Важным элементом поддержания высокого профессионального уровня специалистов в области информационной безопасности Компании является их обучение в специальных учебных заведениях, совершенствование профессиональных навыков, расширение и углубление качества знаний, что достигается участием в тематических мероприятиях, в том числе международных, и целевой переподготовкой на профильных курсах. В 2019 году проведена переподготовка по стандартам ИБ высшего профессионального образования 17 работников Компании. Подготовлено три ведущих аудитора по стандарту ISO 27001:2013.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Подразделения экономической безопасности и противодействия коррупции ПАО «МТС» в 2019 году успешно реализовали комплекс мероприятий, которые позволили обеспечить защиту жизненно важных интересов Группы компаний МТС от внутренних и внешних экономических угроз.

В 2019 году был сделан акцент на реализации следующих направлений развития деятельности:

- содействие повышению эффективности бизнес-процессов и процедур в интересах роста доходности бизнеса при задействовании минимально необходимых барьеров для гарантированного предотвращения потерь и убытков;
- совершенствование механизмов проверки контрагентов;
- развитие устойчивой системы обеспечения кадровой безопасности Компании;
- повышение отдачи от сформированной системы мер по минимизации и возмещению просроченной дебиторской задолженности;
- изучение и применение опыта работы подразделений экономической безопасности других ключевых операторов связи в интересах экономической безопасности Компании.

С целью обеспечения экономической безопасности Компании на 2020 год ставятся следующие первоочередные задачи:

- совершенствование функционала по линии обеспечения внутренней безопасности;
- организация и проведение мероприятий по предотвращению и профилактике коррупционных проявлений;
- анализ и контроль формирования инвестиционных проектов;
- совершенствование проверки контрагентов перед заключением договоров и контрактов;
- проверка кандидатов при приеме на работу;
- участие в мероприятиях по взысканию, минимизации и предотвращению просроченной дебиторской задолженности;
- проверка исполнения договоров, заключенных по результатам закупочных процедур.

В 2019 году повысилась эффективность работы по защите экономических интересов Компании, что, в свою очередь, оказало позитивное влияние на результаты деятельности других структурных подразделений.

На постоянной основе осуществлялось сопровождение процессов закупочной и договорной деятельности, реализации инвестиционных проектов. Сотрудники подразделений безопасности участвовали в качестве экспертов на всех этапах проведения закупочных процедур, что позволило получить существенный экономический эффект.

Осуществлялся сбор информации о юридических лицах, участвующих в процессе проведения закупочных процедур на приобретение товаров, работ и услуг. Одновременно проводился анализ финансово-хозяйственной деятельности потенциальных подрядчиков и делался вывод об их надежности. При получении сведений о наличии проблем у контрагентов (решение о ликвидации, иск о банкротстве, судебные иски и др.) информация передавалась в Блок по управлению закупками. Проблемные контрагенты вносились в «Список проблемных поставщиков», чем блокировалась возможность заключения с ними новых договоров.

Проводилась работа по изучению кандидатов на работу, отклонению тех из них, кто не отвечает предъявленным требованиям, а также является фигурантом Перечня организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму.

Совместно со структурными подразделениями Департамента управления доходами сотрудники подразделений экономической безопасности и противодействия коррупции принимали участие в работе по возмещению просроченной дебиторской задолженности. На постоянной основе осуществлялся контроль и анализ превышения сроков исполнения договорных обязательств. Устанавливалось местонахождение проблемных контрагентов, а при необходимости и их ликвидного имущества.

Проводилась первичная претензионная работа на стадии досудебного переговорного процесса по возвращению проблемной дебиторской задолженности.

Принимая во внимание успешный опыт привлечения подразделений безопасности к возмещению средств Компании, в 2019 году стало развиваться новое направление деятельности — предъявление к вычету НДС при участии сотрудников Департамента.

В 2019 году Департаментом была проведена существенная работа по организации противодействия мошенническим действиям с использованием SIM-карт для получения доступа к дистанционному

банковскому обслуживанию. Реализована эффективная система мер по выявлению и пресечению фактов неправомерной замены SIM-карт у абонентов ПАО «МТС» для последующего хищения денежных средств с их банковских счетов. Был организован постоянный мониторинг с использованием системы Intellinx, позволяющий существенно снизить риски хищения денежных средств с банковских счетов абонентов ПАО «МТС».

Проводилась работа по противодействию коррупции: предупреждение и профилактика коррупционных проявлений, выявление и пресечение коррупционных правонарушений, связанных с причинением как материального, так и имиджевого ущерба Компании.

Работа подразделений безопасности по противодействию коррупции проводилась в тесном взаимодействии с Блоком внутреннего контроля и аудита (БВКА). В рамках Единой горячей линии Группы МТС, куратором которой является БВКА, функционирует Единая горячая линия Блока по корпоративной безопасности и режиму (БКБиР). Сотрудники Компании информируются о существующей возможности сообщать о фактах коррупционных правонарушений.

Особое место занимали мероприятия, проводившиеся подразделениями экономической безопасности и противодействия коррупции совместно с другими функциональными подразделениями Компании, связанные с предупреждением возникновения для Группы МТС финансовых и репутационных рисков.

Для обеспечения максимальной безопасности от этих угроз выстроена слаженная и эффективная система защиты, которая позволяет осуществлять:

- прогнозирование возможных угроз в сфере экономики;
- организацию деятельности по предупреждению возможных угроз;
- выявление, анализ и оценку возникших реальных угроз экономической безопасности;
- принятие решений и организацию деятельности по реагированию на возникшие угрозы;
- постоянное совершенствование системы обеспечения экономической безопасности Компании.

В рамках создания в Компании Единого центра комплексной безопасности получила устойчивое развитие система обеспечения безопасности, внесены улучшения в следующие бизнес-процессы:

- автоматизирован процесс проверки кандидатов и действующих сотрудников на предмет нахождения в Перечне террористов/экстремистов;
- внесены изменения в Кодекс делового поведения и этики;
- организовано взаимодействие с органами государственной власти и управления, реализуется проект автоматизированной системы исполнения запросов правоохранительных органов и суда;
- обеспечена безопасность процессов абонентского обслуживания, соблюдение тайны связи;
- создана база данных для хранения и обмена информацией между подразделениями безопасности Группы МТС;
- реализуется проект автоматизации системы изучения и мониторинга контрагентов совместно с подразделением Big Data с использованием современных подходов и методов, в том числе agile.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛА И ОБЪЕКТОВ

Обеспечение антитеррористической защиты и охраны объектов осуществлялось в соответствии со Стратегией Группы МТС в области обеспечения комплексной безопасности на 2019–2020 годы, а также «Планом мероприятий по обеспечению комплексной безопасности ПАО «МТС» на 2019 год».

Работа по обеспечению пропускного и внутриобъектового режимов в ПАО «МТС» строилась на основании стандарта «Требования по обеспечению безопасности объектов, осуществлению комплексных проверок по вопросам гражданской обороны, чрезвычайным ситуациям и пожарной безопасности на объектах ПАО «МТС». Пропускной режим на объектах Общества осуществлялся сотрудниками ООО «САФЕТИ» с использованием инженерно-технических средств охраны: средствами контроля и управления доступом, систем охранного телевидения, сигнализации, связи, ограждения.

В 2019 году в целях изучения возможности использования функции распознавания лиц для доступа на объекты ПАО «МТС» реализован пилотный проект по распознаванию лиц сотрудников ПАО «МТС» Московского региона.

Для сотрудников Московского региона с июня 2019 года появилась возможность использования смартфона в качестве пропуска с помощью использования сервиса «Мобильный пропуск».

В целях предотвращения фактов вандализма и хищений товарно-материальных ценностей на объектах радиоподсистемы и сохранения бесперебойности услуг связи была продолжена работа по обеспечению непрерывности функционирования наиболее приоритетных БС за счет существенного повышения их оснащенности техническими средствами охраны.

На объектах ПАО «МТС» в течение 2019 года регулярно проводились антитеррористические тренировки и учения с участием работников Компании. Сотрудниками безопасности во всех регионах присутствия ПАО «МТС» осуществлялись объезды базовых станций с целью проверки антитеррористической защищенности.

В соответствии с законодательством Российской Федерации и рекомендациями МЧС России, а также в соответствии с утвержденными Планами мероприятий по вопросам гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности в 2019 году в КЦ и филиалах ПАО «МТС» проведены мероприятия в области ГО и ЧС.

Приоритетные направления в сфере обеспечения безопасности персонала и объектов:

- повышение эффективности работы системы обеспечения безопасности и антитеррористической защиты персонала и объектов ПАО «МТС»;
- обеспечение безопасности руководителей и сотрудников, а также объектов и элементов инфраструктуры ПАО «МТС»;
- реализация мероприятий по предотвращению хищений оборудования и товарно-материальных ценностей с объектов ПАО «МТС»;
- поддержание готовности системы предупреждения и ликвидации чрезвычайных ситуаций ПАО «МТС» к действиям в условиях угрозы и возникновения чрезвычайных ситуаций.