БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

ИТОГИ РАБОТЫ БЛОКА БЕЗОПАСНОСТИ В 2020 ГОДУ И ПЛАНЫ НА 2021 ГОД

Работа Блока безопасности Корпоративного центра ПАО «МТС» (далее Блок безопасности), а также служб безопасности в филиалах и ДЗК ПАО «МТС» в 2020 году была организована и проводилась в строгом соответствии с действующим законодательством Российской Федерации, стратегией, внутренними нормативными документами, планами мероприятий ПАО «МТС».

В соответствии с руководящими документами основные усилия по комплексному обеспечению безопасности в 2020 году были направлены:

- на реализацию задач по обеспечению устойчивости и непрерывности развития бизнеса Группы МТС, выявление и предотвращение рисков в области корпоративной безопасности;
- защиту интересов акционеров, персонала и клиентов Компании, бизнес-процессов, активов, имущества и информационных ресурсов Компании от внутренних и внешних угроз;
- реализацию мер по предупреждению и противодействию угрозам террористического и криминогенного характера;
- совершенствование системы обеспечения экономической безопасности и профилактики коррупции.

В результате проведенных в 2020 году сотрудниками безопасности во взаимодействии с подразделениями Компании проверок и служебных расследований предотвращен ущерб в сумме 2 309,593 млн рублей, установлен ущерб в размере 373,718 млн рублей, возмещен ущерб в сумме 189,149 млн рублей.

В целях недопущения противоправных деяний в сфере закупочной деятельности проведено 53 269 проверок проектов договоров, допсоглашений, заказов, отчетов о выборе поставщика, изучена информация о 36 509 контрагентах, из которых 1366 отклонены как ненадежные.

В процессе изучения кандидатов на вступление в трудовые отношения с Компанией 3763 лицам отказано в приеме на работу по негативным основаниям (как не удовлетворяющим требованиям, предъявляемым ПАО «МТС» к кандидатам, исключая профессиональные качества).

На постоянной основе велась работа по фактам и попыткам краж и порчи имущества Компании, выявлению нарушений требований тайны связи, норм информационной безопасности и соблюдения режима коммерческой тайны.

На основании материалов Блока безопасности (по результатам проверочных мероприятий) в 2020 году правоохранительными органами в отношении лиц, занимающихся противоправной деятельностью и действующих в ущерб корпоративной безопасности ПАО «МТС», возбуждено 333 уголовных дела.

ЗАДАЧИ НА 2021 ГОД

В 2021 году осуществить комплекс мер, направленных на достижение главной цели — обеспечения устойчивости, надежности, непрерывности развития и функционирования бизнеса Компании. Обеспечить последовательную работу в интересах роста доходности бизнеса, создания эффективных барьеров для предотвращения потерь и убытков, противодействия фроду, поддержанию на высоком уровне безопасности персонала и объектов.

\\ 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, невыполнение 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 безопасности информации	Санкции контролирующих органов или отрицательные заключения аудиторов (прокуратура, Минцифры, 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. Несовершенство законодательства по безопасности информации в условиях создания цифровой экономики. Существующий отраслевой подход к регулированию защиты информации не применим при интеграции информации, информационных процессов и систем в целях построения цифровой среды. Наличие в нормативных правовых актах разных требований по безопасности информации к одному объекту защиты создает риск их невыполнения.
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.).
Риск претензий клиентов к защите информации в инновационных продуктах Компании	В предлагаемых потребителям инновационных продуктах необходимо создавать собственную систему защиты информации с учетом актуальных угроз и применимых требований законодательства Российской Федерации. Разработчику продукта требуется высокий уровень компетенции при разработке механизмов защиты информации, чтобы исключить претензии клиентов из-за несоответствия продукта требованиям законодательства или нарушений безопасности информации.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

МИРОВЫЕ ТЕНДЕНЦИИ УГРОЗ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В 2020 году Центром оперативного мониторинга / Security Operations Center (SOC) ПАО «МТС» фиксировались множественные кибератаки на личные кабинеты абонентов ПАО «МТС» и его дочернего общества ПАО «МГТС», а также DDoS-атаки на различные сервисы, включая финтех-ресурс МТС Деньги (payment.mts.ru). Анализ механизмов реализации попыток вредоносного воздействия на абонентов и собственную инфраструктуру информационно-коммуникационных технологий (ИКТ), а также изучение открытых источников показали, что помимо отмечавшегося ранее интереса злоумышленников в получении информационных активов (массивов) с персональными данными и телеметрией потребителей услуг связи, данных финансовых транзакций и иной информации ограниченного доступа отчетливо просматривается тенденция к получению атакующей стороной скрытого параллельного контроля над программными и техническими средствами обработки информации компании-жертвы для их долгосрочной эксплуатации в соответствии со своими целями.

Пандемия COVID-19 также внесла в повестку дня служб информационной безопасности, особенно крупных технологических компаний, новые вызовы в связи с массовым переводом работников на дистанционную форму труда. Хорошо защищенные корпоративные периметры оказались пронизаны тысячами не предусмотренных архитектурой безопасности точек входа с личных устройств работников, которые зачастую не соответствовали корпоративным требованиям к безопасности информации и не были оснащены средствами защиты информации. Отсутствие средств видеоконтроля в местах дистанционного труда работников, имеющих доступ к конфиденциальным сведениям, могло также приводить к снижению уровня безопасности информации, принадлежащей компаниям.

В целом, несмотря на непредвиденные события, вызванные глобальным распространением коронавирусной инфекции и связанными с ними структурными изменениями бизнес-процессов, для корпоративного сектора можно прогнозировать

сохранение в 2021 году актуальности следующих угроз:

- слаженные целенаправленные атаки (Advanced Persistent Threat) на клиентов, онлайн-услуги, ИКТ-инфраструктуру технологических компаний, в том числе для получения информации широкого спектра об архитектуре информационной безопасности существующих экосистем, процессах и мерах ее реализации;
- социальная инженерия и прямая вербовка персонала компаний, особенно находящегося на дистанционной форме труда;
- отсутствие средств управления и контроля личных мобильных средств вычислительной техники работников, обеспечивающих равноценную по функциональности и удобству десктопным платформам защищенную рабочую среду;
- уязвимости нулевого дня в облачных сервисах и услугах, отсутствие механизмов безопасности, приемлемых для крупных компаний;
- ошибки в программном коде коммерческих и собственных ИТ-решений, а также их разработка без учета требований к безопасному производству программного кода;
- формирование бот-сетей на основе оконечного пользовательского оборудования или ИКТ-инфраструктур компаний в целях реализации несанкционированных и зловредных кибератактов;
- несоответствие механизмов защиты в решениях для интернета вещей (IoT) современным угрозам и отсутствие обновлений для устаревших, но находящихся в эксплуатации устройств;
- развитие тенденции усложнения обязательных мер защиты информации на негосударственные информационные ресурсы (персональные данные, профессиональную и коммерческую тайну, сеть связи общего пользования, объекты критической информационной инфраструктуры и др.).

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В МТС

- Защита интересов ПАО «МТС» в информационной сфере достигается комплексом взаимоувязанных организационно-технических мероприятий, образующих единую систему управления и обеспечения информационной безопасности. Комплексный подход позволяет защитить Компанию и ее дочерние общества от современных угроз безопасности информации и инфраструктуре информационно-коммуникационных технологий, обеспечить соответствие законодательным требованиям Российской Федерации, международным стандартам и предотвратить причинение финансового, репутационного и иного ущерба. Система защиты информации построена и развивается с учетом лучших мировых практик, на основе международных стандартов серии ISO 27000 и 15408.
- Система защиты персональных данных обеспечивает третий уровень защищенности в соответствии с требованиями законодательства Российской Федерации.
- Защита тайны связи в сетях связи с встроенными в средства связи механизмами защиты информации соответствует международным стандартам 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, оказывает соответствующие услуги.

РЕЗУЛЬТАТЫ И ДОСТИЖЕНИЯ 2020 ГОДА ПО НАПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Полностью сохранена управляемость подразделениями информационной безопасности при экстренном массовом переводе персонала компании на дистанционную форму работы, и обеспечен непрерывный контроль за соблюдением требований локальных нормативных актов по информационной безопасности.
- Обеспечено развитие систем управления и обеспечения информационной безопасности в соответствии со стратегией Группы МТС в области обеспечения комплексной безопасности на 2019–2020 годы и Планом мероприятий по обеспечению комплексной безопасности ПАО «МТС» на 2020 год. Плановые задачи выполнены, поставленные цели достигнуты.
- Модернизирована системы защиты критичных баз данных, обеспечено WAF-защитой 125 онлайн-сервисов, гарантировано бесперебойное функционирование инфраструктуры открытых ключей и трех удостоверяющих центров ПАО «МТС».
- Осуществлена интеграция процессов обеспечения информационной безопасности в процессы продуктовой трансформации, осуществляется защита экосистемы ПАО «МТС» и сопровождение продуктовых команд.
- Разработана целевая архитектура решения по интеграции дочерних обществ в периметр безопасности ПАО «МТС» и предоставления безопасного контролируемого доступа работникам компаний Группы МТС.
- Организовано постоянное представительство экспертов Департамента информационной безопасности в государственных программах и в рабочих ведомственных группах,

налажено взаимодействие с контролирующими организациями.
- Внедрена система взаимодействия с Главным центром ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) для информирования НКЦКИ (Национальный координационный центр по компьютерным инцидентам) об инцидентах систем КИИ (Критическая информационная инфраструктура) и клиентов коммерческого SOC, субъектов КИИ.
- Британский институт стандартов (British Standards Institution) по результатам надзорного аудита 2020 года подтвердил соответствие Системы менеджмента информационной безопасности ПАО «МТС» международному стандарту ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements и продлил действие Сертификата соответствия № IS719403 на 2021 год. Сертификация расширяет возможности ПАО «МТС» по участию в конкурсах и тендерах, требующих соответствия международным стандартам и практикам ИБ.

РЕЗУЛЬТАТЫ И ДОСТИЖЕНИЯ 2020 ГОДА ПО НАПРАВЛЕНИЮ СОРМ

- 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» продолжаются работы по внедрению специальных комплексов в соответствии с согласованной с ФСБ России концепцией и сроками реализации закона.
- 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 2021 ГОД

- Обеспечение соответствия Системы менеджмента информационной безопасности ПАО «МТС» международному стандарту ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.
- Инфраструктурные изменения ИБ в рамках строительства экосистемы:
  - участие в разработке новых продуктов, услуг и сервисов;
  - обеспечение требований ИБ в процессах производства новых продуктов, услуг и сервисов;
  - переход подразделений ИБ на сервисную модель работы с продуктовыми командами, а также внедрение сервисов ИБ для продуктовых команд;
  - развитие и использование платформ ИБ в дочерних компаниях Группы МТС.
- Развитие продуктов ИБ:
  - расширение услуг Центра оперативного мониторинга / Security Operation Center (SOC);
  - создание платформы киберразведки (Threat Intelligence) для своевременного выявления и предотвращения киберугроз;
  - формирование «красной команды» (Red Team) для выявления кибератак и противодействия им.
- Автоматизация и совершенствование процессов ИБ в части автоматизации процессов формирования соглашения о неразглашении конфиденциальной информации (Non-disclousure agreement — NDA), создание автоматизированной системы конфиденциального электронного документооборота (ЭДО), автоматизация процесса проведения аудитов.
- Выполнение требований законодательства о безопасности критической информационной инфраструктуры и защите персональных данных и развитие системы безопасности значимых объектов КИИ ПАО «МТС».
- Участие в формировании проектов новых нормативно-правовых актов Минцифры России по направлению ИБ.
- Реализация Программы повышения осведомленности персонала в вопросах обеспечения информационной безопасности.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Работа подразделений экономической безопасности и противодействия коррупции ПАО «МТС» в 2020 году была ориентирована на выявление финансово-экономических рисков, предупреждение репутационного и материального ущерба, выработку рекомендаций и принятие мер по их минимизации.

Одно из направлений деятельности — минимизация финансово-экономических рисков при осуществлении контроля выбора поставщиков/подрядчиков, объемов и стоимости оборудования/работ/услуг, исполнения ЛНА Компании.

С целью повышения качества проведения служебных проверок, расследований и претензионной работы с контрагентами по взысканию просроченной дебиторской задолженности в структуре Департамента экономической безопасности и противодействия коррупции ББ КЦ (ДЭБиПК) создан Отдел экономической безопасности.

ДЭБиПК также велась эффективная работа по выявлению нарушений тайны связи абонентов сотрудниками ПАО «МТС». При взаимодействии с правоохранительными органами организована работа по защите тайны связи. Положительные результаты достигнуты при тесном взаимодействии с правоохранительными органами в мероприятиях по выявлению, документированию фактов хищений денежных средств с банковских счетов юридических лиц и пресечению противоправной деятельности.

В связи с изменениями в функциональной стратегии ДЭБиПК произошло перераспределение отдельных функциональных направлений — отдел противодействия абонентскому фроду и его функционал были переданы в АнтифродЦентр ББ КЦ Группы МТС.

С целью сокращения сроков проведения закупочных процедур ДЭБиПК активно участвует в реализации проекта по трансформации закупочной деятельности. Актуализированы регламенты, регулирующие закупочную и инвестиционную деятельности Компании. Новые версии документов устанавливают обязанность закупщиков согласовывать в ДЭБиПК закупочную процедуру, стоимость которой превышает 1 млн рублей, на этапе формирования ТЗ. Внедрен принцип закрепления экспертов ДЭБиПК за конкретными направлениями закупочной деятельности.

ДЭБиПК также проводилась актуализация ЛНА в области обеспечения экономической безопасности и противодействия коррупции. Кардинальные изменения были внесены в регламент процесса РП-053 «Проведение служебного расследования». В результате доработок в новой версии РП формализован процесс проведения служебных проверок.

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ

- Обеспечение контроля закупочной деятельности, инвестиционного планирования, подготовки и реализации инвестиционных проектов по направлениям экономической безопасности и противодействия коррупции.
- Совершенствование организации обеспечения экономической безопасности и противодействия коррупции в Группе МТС.
- Участие в разработке и реализации стратегии Группы МТС в области обеспечения комплексной безопасности Группы МТС.
- Организация и контроль за своевременной разработкой и актуализацией ЛНА в области обеспечения экономической безопасности и противодействия коррупции.
- Методологическое руководство, контроль и координация деятельности региональных и дочерних подразделений экономической безопасности и противодействия коррупции.

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 2020 год».

- Работа по обеспечению пропускного и внутриобъектового режимов в ПАО «МТС» строилась на основании стандарта «Требования по обеспечению безопасности объектов ПАО «МТС». Пропускной режим на объектах Компании осуществлялся сотрудниками ООО «САФЕТИ» с использованием инженерно-технических средств охраны, средств контроля и управления доступом, систем охранного телевидения, сигнализации и связи.
- В 2020 году в рамках инвестиционного проекта реализована возможность использования функции распознавания лиц для доступа на объекты ПАО «МТС» Московского региона.
- Возможность использования смартфона в качестве пропуска с помощью сервиса «Мобильный пропуск» в 2020 году реализована в нескольких регионах.
- В целях предотвращения фактов вандализма и хищений товарно-материальных ценностей на объектах радиоподсистемы и обеспечения бесперебойности услуг связи продолжена работа по обеспечению непрерывности функционирования приоритетных БС за счет существенного повышения их оснащенности техническими средствами охраны.
- В целях проверки готовности сотрудников охраны ЧОП к действиям при возникновении чрезвычайных происшествий на объектах ПАО «МТС» в течение 2020 года совместно с работниками Административного блока проводились противопожарные и антитеррористические тренировки. Сотрудниками безопасности во всех регионах присутствия ПАО «МТС» осуществлялись объезды базовых станций с целью проверки их антитеррористической защищенности.
- В 2020 году на плановой основе проводились мероприятия, направленные на выявление и устранение возможных каналов утечки речевой информации, циркулирующей в помещениях руководства Компании по акустическим и техническим каналам.
- 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 2020 году в Группе МТС проведены мероприятия по данному направлению.

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛА И ОБЪЕКТОВ

- Повышение эффективности работы системы обеспечения безопасности и антитеррористической защиты персонала и объектов 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.