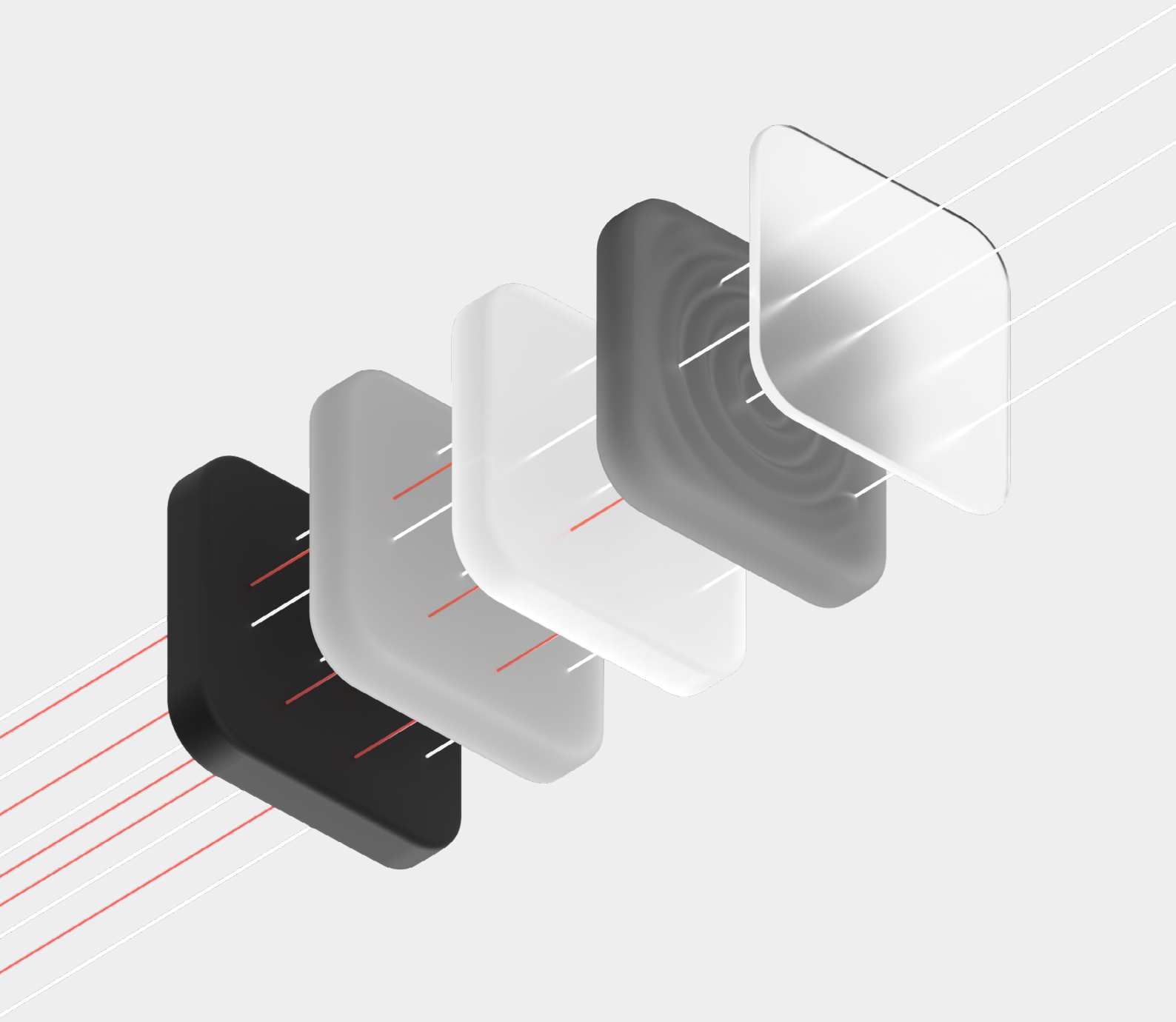
Основные меры по информационной безопасности, применяемые в компании Yandex Cloud



Yandex Cloud

2022

Оглавление

Термины и определения

Компания — Общество с ограниченной ответственностью «Yandex Cloud».

Клиент — учреждения, предприятия, организации любых форм собственности, а также физические лица, использующие Yandex Cloud.

Сотрудник — физическое лицо, состоящее в трудовых отношениях с Компанией на основании трудового договора, который предусматривает применение Положения о коммерческой тайне.

Конфиденциальная информация — сведения любого характера, включая техническую, организационную, технологическую, производственную, финансово-экономическую и/или иную информацию, в том числе данные:

о результатах интеллектуальной деятельности в научно-технической сфере;

о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность для Компании и/или любой компании группы лиц Яндекс в силу неизвестности ее третьим лицам, к которым нет свободного доступа на законном основании и в отношении которых Компанией в соответствии с Положением о коммерческой тайне введен режим конфиденциальности (коммерческой тайны).

третьих лиц, которые были переданы Компании на законном основании и составляют коммерческую тайну.

Общие положения

В Компании информация клиентов и служебных сервисов является ценным ресурсом. Конфиденциальность, целостность и доступность информационных активов имеют важное значение для конкурентоспособности Компании на рынке, соблюдения законов Российской Федерации и поддержания коммерческого имиджа. Обеспечивать безопасность информационных активов — первостепенная задача в деятельности Компании.

В Компании внедрена Система управления информационной безопасностью (СУИБ) в отношении процесса предоставления сервисов. СУИБ определяет процессы безопасной разработки, правила установки обновлений программного обеспечения (ПО), действия при возникновении инцидентов.

Организация физической безопасности

В Компании, включая дата-центры, действует пропускной и внутриобъектовый режимы, которые нужны, чтобы обеспечить безопасность жизни и здоровья сотрудников и посетителей, сохранность товарно-материальных ценностей и оборудования, а также не допустить хищения, чрезвычайные ситуации и террористические акты.

Доступ на территорию дата-центра строго регламентирован. Гостям и сотрудникам Компании, которые не работают в дата-центре постоянно, нужна заранее одобренная заявка.

Объекты облачных сервисов (стойки, железные ящики, зона диагностики) находятся под постоянным видеонаблюдением.

Записи видеокамер хранятся на серверах Яндекса в оперативном доступе не менее трех месяцев.

Сотрудники службы безопасности следят за доступом в защищенные зоны и к стойкам сервиса.

Вышедшее из строя оборудование заменяется только по заявке. При выводе оборудования из эксплуатации или его повторном использовании данные с носителей удаляются.

Неисправное оборудование хранится в сейфах в специальной упаковке. Оборудование не выносится из помещений без одобренной заявки.

Если для работы необходимо привлечь внешних исполнителей, их визит на протяжении всего времени обязательно должен проходить в сопровождении сотрудника, которому разрешен доступ к оборудованию Компании.

В Компании действует политика чистого стола и чистого экрана. Это нужно, чтобы не допустить компрометацию или кражу информации из оставленных без присмотра ценных документов или незаблокированных рабочих ноутбуков.

Управление доступом

В Компании действует Политика управления доступом, которая содержит требования к организации доступа сотрудников к серверам, виртуальным машинам и сервисам. Политика обязательна для исполнения всеми сотрудниками, участвующими в предоставлении сервисов Компании.

Аутентификация во внутренних интерфейсах осуществляется через внутренний Паспорт (passport.yandex-team.ru) или средствами системы, которой принадлежит административный интерфейс.

После увольнения сотрудника доступ к внутренним интерфейсам прекращается.

Соблюдение политики доступа к служебным интерфейсам контролирует служба информационной безопасности (ИБ) .

Административный доступ на серверы по SSH-ключу осуществляется только через специализированный сервис контроля доступа Бастион (класс PAM). Все SSH-ключи защищены аппаратными токенами (Yubikey).

Доступ во внутреннюю сеть осуществляется через 802.1X или VPN.

При доступе во внутреннюю сеть оборудование аутентифицируется при помощи сертификатов.

Также в Компании регламентированы требования к сложности и использованию паролей (политика паролей).

Охрана конфиденциальности

Компания не раскрывает информацию третьим лицам, за исключением тех случаев, когда это предусмотрено действующим законодательством или положениями договора. По возможности Компания перенаправляет запрос третьей стороны клиенту.

В отношении Конфиденциальной информации Компания устанавливает следующие меры:

- определять перечень сведений, составляющих коммерческую тайну Компании, утверждая его приказом по Компании;
- ограничивать доступ к Конфиденциальной информации, ее передаче и предоставлению, устанавливая порядок обращения с этой информацией и осуществляя контроль за соблюдением этого порядка;
- постоянно мониторить подозрительную активность (изменение файлов операционной системы и конфигурации, обмен данными по сети и т.д.), происходящую в корпоративных ресурсах Компании, в том числе на рабочем устройстве Сотрудника;
- отслеживать лиц, которые получают доступ к Конфиденциальной информации и (или) лиц, которым предоставлялась такая информация;

регулировать отношения по использованию Конфиденциальной информации в соответствии с Положением о коммерческой тайне, включая отношения с сотрудниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

наносить на Документы, Электронные документы и иные материальные носители, а также включать в состав реквизитов любых документов, гриф.

Процесс безопасной разработки

В Компании реализованы и постоянно развиваются ключевые компоненты процесса безопасной разработки (Security Development Lifecycle, SDLC).

Проводится регулярное информирование сотрудников, которые занимаются разработкой облачных сервисов.

Оно включает в себя:

Обязательный ежегодный тренинг для всех специалистов. Все разработчики сдают теоретический и практический тесты.

Знакомство с внутренним руководством. В нем описаны базовые принципы безопасной разработки, перечень возможных уязвимостей для разного типа приложений, показаны типичные примеры уязвимого кода и исправлений. Также в нем есть информация о том, как использовать технологии, снижающие вероятность эксплуатации уязвимости (mitigations). Регламенты указывают минимальные требования к использованию криптографии, которым необходимо следовать при разработке сервисов и приложений.

Постоянный обмен знаниями с экспертами.

Ежегодная игра Capture The Flag. Тренинг помогает командам избегать ошибок при проектировании и разработке реальных сервисов.

В Компании внедрено архитектурное планирование. Перед созданием любого продукта и до изменения архитектуры действующего сервиса проводятся совещания с экспертами в области безопасности, на которых рассматриваются возможные угрозы и способы атак на сервис. Совместно с другими мерами Defense in Depth это обеспечивает надежную защиту сервиса и обрабатываемых данных.

Проводится статический и динамический анализ. Системы статического анализа кода регулярно сканируют репозитории в процессе раз-

работки. Проверяется качество кода, покрытие кода тестами. Команды также используют инструменты динамического анализа для sanity- и fuzzy-тестирования.

Внедрена процедура финального тестирования по методологии белого ящика, которая проводится перед каждым крупным этапом проекта. Например, перед выходом сервиса в Preview. Проверяется не только сам сервис, но и окружение, в котором он функционирует.

В Компании разделены среды разработки, тестирования и промышленной эксплуатации, а также внедрена система контроля, которая не позволяет реплицировать данные из промышленного контура в другие окружения.

Управление обновлениями

В Компании регламентируется максимальный срок установки для каждого вида ПО. Устанавливать обновление, выпущенное производителем программы, необходимо в рамках этого срока.

Управление уязвимостями

Компания регулярно проводит проверку уязвимостей предпроизводственных серверных систем с выходом в интернет и сетевых устройств перед их перемещением в промышленный контур. Все уязвимости устраняются до перемещения.

При обнаружении уязвимостей в компонентах промышленной среды проводится анализ сложности эксплуатации и серьезности последствий. После этого команда разработки готовит обновление с учетом найденных недочетов.

Закрытие уязвимостей выполняется по планам и в соответствии с внутренними требованиями. Иногда могут выпускаться аварийные обновления, требующие исправления до планового периода обслуживания. В этом случае развертывание аварийных обновлений может происходить в соответствии с планом, согласованным с бизнес-департаментом.

Непрерывность бизнеса и отказоустойчивость

В Компании реализована система управления непрерывностью бизнеса, которая определяет требования ко всем критичным процессам.

Нарушение этих требований влияет на выполнение обязательств перед партнерами и клиентами.

Эта система состоит из планов, в которых описана последовательность действий сотрудников в возможных негативных сценариях. Она предусматривает механизмы резервирования для всех критичных компонентов облачной платформы, включая георезервирование в трех географически распределенных дата-центрах.

Для проверки эффективности планов регулярно проводятся тестирования. Результаты тестирования анализируются, вырабатываются меры по устранению недостатков, и принимается решение о пересмотре существующих планов.

В Компании действует политика резервного копирования. Она определяет основные подходы к созданию, хранению и восстановлению резервных копий данных, которые необходимы для непрерывного оказания услуг при выходе из строя оборудования или при сбоях в работе ПО. Для информации пользователей, размещенной в сервисах PostgreSQL, MySQL, MongoDB, ClickHouse, Redis, выполняется резервное копирование. Файлы бекапов шифруются. Возможность восстанавливать информацию из бэкапов регулярно проверяется на тестовых базах данных, размещенных в Облаке, не реже 1 раза в месяц.

Управление персоналом

Компания проверяет на благонадежность всех кандидатов перед их трудоустройством.

Сотрудники знакомятся с требованиями внутренней политики и регламентов, включая «Политику информационной безопасности» и «Положение об обработке персональных данных».

Сотрудники дата-центров, администраторы и разработчики на регулярной основе проходят дополнительные курсы, связанные с безопасной разработкой и регламентами администрирования и эксплуатации облачных сервисов. Обучение проходит очно и онлайн.

После обучения сотрудники проходят тестирование, подтверждающее уровень знаний.

Результаты проверки практических навыков и теоретических знаний анализируются. По итогам тестирования система обеспечения ИБ компании корректируется.

Сотрудники, не прошедшие обучение в установленный срок, не допускаются к работе.

Управление инцидентами

В Компании внедрен процесс управления инцидентами ИБ, который осуществляется Центром операционной безопасности (Security Operations Center, SOC) в составе Службы информационной безопасности ООО «Яндекс».

Сбор событий информационной безопасности ведется с помощью:

- автоматических мониторингов инфраструктуры Yandex Cloud;
- HIDS (система выявления аномальной активности собственной разработки) и иных агентов ИБ;
- средств контроля приложений и применения политики безопасности на уровне приложений (AppArmor, seccomp);
- настроенной отправки регистрируемых событий в SIEM (SSH, sudo, логов приложений и т. д.);
- дежурных по информационной безопасности в рамках действующего процесса;
- дежурных по сервисам в рамках действующего процесса;
- технической поддержки Компании.

Для типовых инцидентов ИБ разработаны планы реагирования.

Если инцидент ИБ не типовой, дежурный по ИБ разрабатывает оперативный план реагирования.

Приоритеты инцидентов ИБ:

- **Very High** — инцидент затрагивает всех пользователей Yandex Cloud, есть существенная угроза или произошло существенное нарушение конфиденциальности, целостности и доступности данных пользователей сервиса.
- **High** — инцидент приводит или привел к существенной деградации Yandex Cloud, приводит или привел к нарушению целостности, конфиденциальности и доступности сервиса или данных существенной части его клиентов.

Medium — инцидент серьезно влияет или повлиял на безопасность Yandex Cloud и данные пользователей.

Low — инцидент незначительно повлиял или влияет на безопасность Yandex Cloud.

Very Low — инцидент незначительно повлиял на платформу, влияния на клиентов нет.

Безопасность инфраструктуры облачной платформы

Безопасность машин облачной платформы

Безопасность физических и сервисных виртуальных машин обеспечивается на нескольких уровнях.

Типы межсетевых экранов на уровне сети:

фильтры пакетов на границах внутренних подсетей;

простой фильтр пакетов на уровне Top-of-Rack коммутатора;

аппаратный межсетевой экран на границе инфраструктуры Яндекса и инфраструктуры Yandex Cloud;

программный межсетевой экран, установленный на всех физических хостах и виртуальных машинах.

В Компании используются дополнительные средства защиты:

AppArmor и Seccomp — формируют среду изоляции (песочницу) для приложений. Все виртуальные машины на уровне хостовой операционной системы работают под AppArmor.

Osquery 4 — реализует функционал Host-based Intrusion Detection System, собирает телеметрию с хоста, включая логи AppArmor и Seccomp, обогащает их и отправляет во внутреннюю Security Information and Event Management (SIEM).

Система мониторинга и оповещения о подозрительном поведении.

Конфигурации операционных систем описаны кодом и хранятся в репозитории. Все изменения конфигураций проходят обязательную проверку в тестовых средах перед переносом в продуктивную среду.

В Компании действует политика защиты от злонамеренного кода. Она применяется ко всем системам, подверженным вирусным заражениям.

Разделение и изоляция ресурсов

Административные и пользовательские ресурсы в Компании изолированы. Физическая изоляция с помощью групп хостов. Критичные с точки зрения безопасности сервисы запускаются в виртуальных машинах на отдельной группе физических хостов, на которой не запускаются пользовательские виртуальные машины.

Логическая изоляция на уровне гипервизора и отдельных ядер. Логическая изоляция осуществляется с помощью сервиса Identity and Access Management (IAM). Все административные операции проводятся через IAM. Для их выполнения нужны специальные права, недоступные пользователям Компании.

Изоляция на уровне сети. Все административные виртуальные машины запускаются в физически или логически изолированных сетях. Корпоративная сеть провайдера отделена от сети облачной платформы. Доступ контролируется автоматически с помощью динамических и хостовых межсетевых экранов и списков управления доступа на маршрутизаторах.

В мультитенантных системах изоляция реализуется на уровне приложения. Также она происходит с помощью проверки прав доступа к Yandex Cloud и каталогу пользователя, осуществляющего операцию над ресурсами.

Защита от атак на цепочку поставок (supply chain attacks)

Подразделение Яндекса Research and Development (RnD) занимается проектированием и организацией производства серверного оборудования, которое используется в Компании. Все серверное оборудование проходит тестирование перед вводом в эксплуатацию. Пакеты с кодом, которые внедряются в продуктивную среду, содержат криптографическую подпись. «Пакетный менеджер» проверяет ее перед установкой. Все пакеты сторонних производителей ПО с открытым исходным кодом переподписываются перед добавлением в репозиторий пакетов компании.

Релиз обновлений происходит со специальных серверов управления, доступ к которым возможен только через описанный выше Бастион. Журнал обновления продуктивной среды сохраняется и анализируется релиз-инженером. Все изменения в приложениях и конфигурации проходят обязательную проверку.

Защита и удаление данных

Компания использует размещенную клиентом информацию только для выполнения целей договора и уведомляет клиента об инцидентах, которые затрагивают пользовательские данные. Владельцем данных всегда является пользователь облачной платформы.

Удаление данных выполняется по сценариям:

Удаление ресурса при получении запроса через API сервиса. Если сервис получает запрос на удаление ресурса через API, ресурс сразу помечается как удаляемый.

Автоматическая блокировка облака. По истечении 60 дней (при блокировке профиля из-за нарушения условий использования — 7 дней) Компания может пометить ресурсы как удаляемые.

Удаление профиля пользователя. Если профиль не был восстановлен в течение 30 дней после удаления, ресурсы во всех сервисах помечаются как удаляемые. При разрыве контракта весь профиль пользователя и ресурсы в нем сразу помечаются как удаляемые.

Ресурс, помеченный как удаляемый, не может быть восстановлен. Фактическое удаление производится в течение 72 часов.

Криптографическая защита

Способы криптографической защиты пользовательских данных:

Шифрование на уровне Storage. Storage — мультитенантная система, в которой данные шифруются отдельным набором ключей перед их записью на физический диск. Ключи шифрования хранятся на физических хостах, на которых работает Storage.

Шифрование на уровне баз данных Yandex Database (YDB). В YDB реализовано шифрование на уровне баз данных. Данные шифруются непосредственно перед отправкой в Storage (например, в Yandex Message Queue).

Шифрование резервных копий данных в Managed Services for Databases (MDB). Все резервные копии, создаваемые сервисами MDB, шифруются перед отправкой в постоянное хранилище. Для каждого пользователя генерируется пара ключей ассиметричного шифрования, которая хранится в зашифрованном виде во внутренней инфраструктуре MDB. При разворачивании базы данных из резервных копий используется приватная часть,

которая удаляется из виртуальной машины сразу после использования.

Шифрование данных при передаче. Для шифрования данных при передаче используется протокол TLS. Ключи для работы протокола TLS хранятся на хостах, на которых он используется. Все leaf-TLS ключи должны создаваться со сроком действия не более одного года. Intermediate-сертификаты должны иметь срок действия не более пяти лет, Root-сертификаты могут иметь срок действия до 20 лет. Допускается автоматизация ротации ключей TLS (например, при помощи сервиса Certificate Manager).

Криптографические ключи также могут использоваться:

- для реализации межсервисной аутентификации;
- в качестве ключей подписи cookie и IAM-токенов (учетные данные пользователей для доступа к ресурсам Облака).
- как SSH. Управление ключами SSH производится сотрудниками самостоятельно. Для целей SSH-PKI используется X.509 сертификат, который хранится на Yubikey. Долговременные ключи должны иметь срок действия не более одного года, а сессионные ключи — не более 24 часов.
- для сервиса Key Management Service (сервис хранения и управления ключами шифрования данных пользователей).

В сервисе KMS хранятся ключи пользователей, а также мастер-ключ для их шифрования. Для шифрования ключей KMS применяются алгоритмы AES-128/AES-192/AES-256 в режиме GCM. Ключи пользователей не покидают периметр сервиса KMS в открытом виде, мастер-ключ сервиса KMS шифруется при хранении с помощью TPM.

Пользователи сами управляют политикой ротации ключей KMS. Срок ротации мастер-ключа — пять лет.

Длина ключа симметричного шифрования, ключей хэш-функций составляет не менее 128 бит. Длина ассиметричных ключей RSA составляет не менее 2048 бит. Для других ассиметричных алгоритмов длина ключа должна быть такой, чтобы количество классов эквивалентных ключей было не менее чем 2^{128}.

Компрометация ключей рассматривается как инцидент информационной безопасности в соответствии с Регламентом обработки инцидентов ИБ.

Ответственность за корректность реализации схем шифрования и своевременную ротацию ключей возлагается на руководителей соответству-

ющих сервисов. Ответственным подразделением Компании проводятся периодические проверки выполнения указанных выше требований в рамках процессов SSDL и внутреннего аудита.

Внутренний и внешний аудиты, тесты на проникновение

Чтобы проверить работоспособность действующих процессов ИБ и их развитие, Компания проводит периодические внутренние и внешние аудиты и тесты на проникновение.

СУИБ проходит регулярный внутренний аудит с учетом рекомендаций ISO 19011.

В рамках внутреннего аудита проверяются управление активами, физическая безопасность, управление изменениями и инцидентами ИБ, мониторинг, другие процессы, а также группы контроля ИБ.

Согласно законодательству в области защиты персональных данных (ПДн) и стандартам ISO, в компании есть план внешних аудитов на соответствие требованиям ISO 27001, ISO 27017, ISO 27018, а также план контрольных мероприятий для проверки соответствия процессов и контроля ИБ приказу ФСТЭК №21.

Компания использует практики Red Teaming. Уязвимости, найденные благодаря регулярным тестам, исправляются командами разработки или, если невозможно оперативно выпустить обновление, закрываются компенсирующими мерами до выхода исправления.