

Selectel

Как построить защищенные информационные системы

Содержание

Когда важно защищать информационную систему	3
Три главных требования информационной безопасности	4
Конфиденциальность.....	4
Доступность.....	5
Целостность.....	6
Требования законодательства в сфере ИБ	7
Как оценить риск от ИБ-угрозы для конкретной компании	8
Оценка рисков: прямые потери.....	8
Оценка рисков: имиджевые потери.....	9
Преимущества IaaS перед локальными ИБ-решениями	10
Услуги Selectel в сфере ИБ	11
О Selectel.....	11
Инфраструктурные решения.....	11
Дополнительные сервисы для защиты инфраструктуры.....	12
Почему Selectel.....	13
Примеры кейсов	15
Платежный сервис.....	15
Медицинская лаборатория.....	15
Туристический оператор.....	15

Когда важно защищать информационную систему

Информационные системы (далее ИС) – неотъемлемая часть бизнес-процессов, они есть в любом бизнесе. Например, это системы финансовой отчетности, мониторинга, управления, логистики и многие другие. Специалисты по информационной безопасности (далее ИБ) защищают данные систем от хищений/изменений как случайного, так и умышленного характера – DDoS-атак, внутренних угроз, атак злоумышленников.

Со временем варианты кибератак развивались в связи с усложнением информационных систем, что приводило все к большему урону для бизнеса. В среднем, число выявленных инцидентов в сфере ИБ увеличивается на **66% ежегодно**. 2018 год не стал исключением **по росту внешних и внутренних угроз ИБ**, а в чем-то перекрыл показатели прошлых лет. Поэтому вопрос защиты информационных систем – обязательная составляющая любого бизнеса.

В настоящем материале рассмотрим:

- инструменты информационной безопасности, которые рекомендованы каждому бизнесу;
- требования законодательства РФ, что действуют для компаний и их влияние на ИБ;
- влияние отраслевой специфики компании и риска угроз на индивидуальные требования к защите ИС.



«Вопрос защиты информационных систем – обязательная составляющая любого бизнеса»

Три главных требования информационной безопасности

Частые типичные проблемы с информационной безопасностью привели к тому, что разрозненные требования к ИБ стали складываться в конкретно сформулированные стандарты.

Ключевые требования к информационной безопасности для любого бизнеса

Конфиденциальность — обеспечение доступа к информации только авторизованным пользователям. Всем компаниям необходимо обеспечивать сохранность своих данных.

Доступность — обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости (то есть, требование в любых условиях предоставить легитимным пользователям доступ). Особенно важно для компаний, которые ведут через глобальную сеть свой бизнес или часть бизнес-процессов, например, коммуникацию.

Целостность — обеспечение достоверности, полноты информации и методов ее обработки. Критичное требование для систем обработки информации, например, аналитических систем или систем обработки данных, СУБД.

Конфиденциальность

Безопасность данных и конфиденциальность пользователей являются одними из главных приоритетов информационной безопасности. Постоянный рост количества и разновидностей угроз диктует возведение конфиденциальности данных информационной системы в формат стандарта и непреложного требования при построении IT-инфраструктуры компании.

Известные случаи

- Маркетинговая компания Exactis (США). Произошла [утечка базы данных](#) ElasticSearch размером 2 терабайта, содержащей более 340 млн записей. Из них около 230 млн — персональные данные физических лиц, 110 млн — контакты различных организаций. Утечка стала возможной ввиду отсутствия защиты базы данных.
- Индексация документов Google поисковой системой Яндекс. Нашлось довольно много [критичной информации](#), по незнанию или халатности опубликованных пользователями, в том числе юридическими лицами, без надлежащего контроля.

Решение

Безопасность бизнес-процессов и информационных активов компании должна быть основана на следующих инструментах:

- надежное хранение данных,
- средства защиты для повышения уровня безопасности сетей информационных систем,
- дополнительные средства защиты для повышения безопасности сети, операционных систем и баз данных.

Доступность

Большинство сайтов легко вывести из строя, а это влечет финансовые и репутационные потери. Доходы киберпреступников во всем мире составляют не менее [1,5 триллиона долларов](#) (российский ВВП в 2018 году – 1,58 триллиона долларов). Россия входит в десятку [стран-лидеров](#) по числу DDoS-атак. Кроме DDoS – атак, связанных с движением «хактивизм» или политическими [акциями](#), также развито так называемое DDoS-вымогательство. Например, [PumpWaterReboot](#) требовали выкуп у десятка российских банков, издательских домов и не только. Когда какой-то ресурс – важный актив компании, то его простой недопустим для бизнеса. Поэтому требование соблюдать доступность информационной системы при любых обстоятельствах стало, можно сказать, стандартом.

Известные случаи

- В марте 2018 года была зафиксирована DDoS-атака мощностью 1,7 терабита в секунду. Хакеры [попытались вывести из строя системы](#) одного из крупных американских сервис-провайдеров.
- В конце 2018 года у Росреестра [произошел технический сбой](#): на несколько дней был закрыт доступ к сервису выдачи выписки из Единого государственного реестра недвижимости. Сервис был отключен в связи с необходимостью устранения угроз, вызванных DDoS-атаками.
- Зачастую хакеры не ограничиваются угрозами – иногда атаки можно наблюдать практически в прямом эфире, что [произошло](#) с почтовым сервисом VFEMail. Сервис основан в 2001 году жителем США, и с тех пор обслуживал частных клиентов (бесплатно – 50 мегабайт для писем) и организации на их собственных доменах. В 2015 году сервис упоминался наряду с сервисом защищенной почты ProtonMail как жертва вымогателей – владелец сервиса цитировал требование организаторов DDoS-атаки выплатить пять биткоинов. 11 февраля без предварительных угроз злоумышленники стерли информацию со всех основных и резервных серверов VFEMail, буквально за несколько часов уничтожив бизнес компании почти полностью.

Решение

Основные угрозы корпоративным сетям – это атаки злоумышленников и техногенные/природные катастрофы. Именно поэтому наиболее приоритетными инструментами будут являться:

- защита от DDoS-атак,
- WAF – защита веб-приложений,
- построение катастрофоустойчивых систем.

Целостность

Только надлежащая защита позволит сохранить информацию без искажений, поэтому целостность информации (данных) является одним из важных требований информационной безопасности. По характеру нарушения целостности рассматривают:

- саботаж – повреждение, наступившее в результате целенаправленных злонамеренных действий (атаки хакеров, деятельность сотрудников, решивших по разным причинам расстроить функционирование компании, встречаются и ситуации, обусловленные корыстными мотивами, местью участников и т.п.);
- сбой программ – повреждение, связанное с некорректной настройкой приложения, взломом или действиями вредоносных программ (следует отметить, по мере увеличения способов хранения, обработки, записи данных будет возрастать и количество рисков).

Решение

Существуют специальные средства контроля целостности для защиты на уровне приложений, операционной системы, сетей. Они также могут распознать несанкционированный доступ к данным: если после проверки по заданным алгоритмам система выявит несоответствия, сработает уведомление для администратора или система автоматически выполнит нужное действие (закроет доступ, сохранит изменения файла, вернет файл в исходное состояние). Для передачи данных во внешние информационные системы используют шифрование и другие средства криптографии. Чтобы информация сохранялась в неизменном виде в случае ошибок хранения/обработки, вредоносного ПО, отказа оборудования или человеческой неосторожности, применяют также резервное копирование. В таком случае данные можно восстановить из резервных копий (хранить которые желательно на разных устройствах и удаленных защищенных площадках). Таким образом, для соблюдения целостности применяют:

- системы контроля целостности/ мониторинга актуальности данных,
- обеспечение резервирования информационных активов,
- защищенные дата-центры и каналы связи.



Требования законодательства в сфере ИБ

На начало 2019 года существует ряд требований законодательства, которые действуют для российских компаний. Кроме большого количества отраслевых стандартов существуют требования, распространяющиеся на большинство коммерческих компаний. В первую очередь, это требования по защите персональных данных:

- [№ 152-ФЗ](#),
- [№ 149-ФЗ](#),
- [постановление Правительства № 1119](#),
- [приказ ФСБ РФ № 378](#),
- [приказ ФСТЭК № 21](#).

Соответствие требованиям законодательства проверяется контролирующими органами и регуляторами — государственными службами, уполномоченными проводить проверки в части соблюдения законодательства о персональных данных. Это Роскомандзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций), ФСТЭК (Федеральная служба по техническому и экспортному контролю) и ФСБ (Федеральная служба безопасности). При этом Роскомнадзор проверяет правовые основания обработки персональных данных, не проверяя состояние технической защиты и предпринимаемые технические меры по защите ИС персональных данных. Если поступают жалобы, то возможны и внеплановые проверки.

[Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных](#)

Оператор персональных данных

Оператор — юридическое или физическое лицо, государственный орган, муниципальный орган, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Оператору персональных данных необходимо проводить оценку эффективности принимаемых по защите мер не реже одного раза в 3 года — самостоятельно или с привлечением подрядчика, у которого имеется лицензия на деятельность по технической защите конфиденциальной информации.

Как оценить риск от ИБ-угрозы для конкретной компании

Отраслевая специфика компании влияет на возможные ИБ-угрозы. Например, для мерчант-компаний (платежных шлюзов) они будут заключаться в краже денежных средств, для рекрутингового агентства — базы данных. Поэтому стоит учесть индивидуальные требования к защите ИС, согласно степени влияния конкретного риска на бизнес.

Оценка рисков: прямые потери

Подсчет величины финансовых потерь помогает осознать важность защиты информационной системы от конкретного вида угроз. Оценка рисков также помогает расставить приоритеты в очередности реализации подсистем информационной безопасности — что стоит внедрить в первую очередь, а какое решение не столь критично. С помощью схемы ниже рассчитайте среднегодовые потери в случае реализации угрозы (оценку стоит производить в отдельности по каждому типу инцидентов). Для оценки могут использоваться данные отраслевых отчетов или собственные исторические данные компании об инцидентах.

В общем случае в расчете на год:

$$\begin{aligned} & \text{Ущерб от реализации угрозы (ожидаемые потери)} = \\ & = \text{Потенциальный ущерб от единичной угрозы} \times \text{Частота возникновения подобных угроз} \end{aligned}$$

Потенциальный ущерб от единичной угрозы рассчитывается как произведение ценности актива на процент потерь, которые возникнут вследствие реализации характерной угрозы.

$$\begin{aligned} & \text{Потенциальный ущерб от единичной угрозы} = \\ & = \text{Ценность актива} \times \text{Процент потерь от угрозы} \end{aligned}$$

Пример

Рассчитаем риски на примере интернет-магазина. Допустим, веб-приложение интернет-магазина обрабатывает персональные данные клиентов.

Ценность актива (объем базы персональных данных) можно рассчитать различными способами, в нашем примере посчитаем ценность базы данных как суммарные затраты на ее создание (сколько компания потратила средств на составление этой базы). В среднем, стоимость привлечения одного клиента составила 3,7 тысяч рублей, с учетом всех маркетинговых активностей. Всего в базе две тысячи клиентов.

$$\text{Ценность актива} = 3\,700 \text{ руб.} \times 2\,000 = 7\,400\,000 \text{ руб.}$$

Допустим, что после взлома уходит 5% клиентов (например, база может быть передана конкурентам или общественности станет известно об утечке).

$$\text{Процент потерь от угрозы} = 5\%$$

Следовательно:

Потенциальный ущерб от единичной угрозы = 7,4 млн руб. × 5% = 370 000 руб.

Если веб-приложение обрабатывает персональные данные, их [утечка возможна в 18% случаев \(данные за 2018 г.\)](#). В таком случае:

Частота возникновения подобных угроз = 0,18

Таким образом:

*Ожидаемый среднегодовой ущерб от потери данных =
= 370 000 руб. × 0,18 = 66 600 руб.*

Если стоимость применения средств защиты веб-приложения будет меньше ожидаемого ущерба в случае реализации угрозы, это станет аргументом к их внедрению.

Похожая логика оценки пригодится для анализа любой конкретной угрозы. Условно, чем больше компания тратит на создание и поддержку актива, к которому применимы угрозы в сфере информационной безопасности, тем качественнее этот актив стоит защищать.

В указанном выше примере не учтено то, что в случае утечки данных сам магазин может остановить работу на какое-то время, чтобы устранить уязвимость. За это время компания не сможет принимать часть заказов, что скажется на выручке, не говоря об имиджевых потерях.

Оценка рисков: имиджевые потери

Помимо прямых потерь вследствие атак, простоя, утери, кражи той или иной информации, существуют репутационные потери, которые подсчитать довольно сложно, но важно. Репутационные потери отразятся на деятельности компании — как одномоментно, так и в перспективе. Это обернется снижением лояльности клиентов и бизнес-партнеров; на компанию могут быть возложены крупные штрафы или судебные иски; возможно даже полное закрытие бизнеса.

Примеры

- Сервис электронной почты VFEmail [подвергся атаке](#), в результате которой все данные были удалены — все, что нажато непосильным трудом за 18 лет существования компании, включая резервные копии. Хакер отформатировал все серверы компании, включая те, на которых хранились бэкапы.
- Сервис по продаже концертных билетов Ticketfly, сообщил о [хакерской атаке](#) на свою базу данных. База содержала персональные данные миллионов клиентов сервиса. Она была похищена злоумышленником, требовавшим за возврат выкуп в биткоинах.
- Управление комиссара по информации Великобритании [оштрафовало Facebook](#) на 500 тысяч фунтов (около 644 тысяч долларов) из-за утечки персональ-

ных данных миллионов пользователей из-за действий компании Cambridge Analytica. Штраф мог бы достигнуть 4% оборота (1,9 миллиарда долларов), если бы было доказано, что утечка произошла после принятия закона о GDPR.

Статистика довольно неутешительная, поэтому необходимо интегрировать решения по ИБ в бизнес-процессы, использовать средства предотвращения и снижения рисков, в том числе, размещая объекты своей инфраструктуры в доверенных областях и надежных ЦОД.

Преимущества IaaS перед локальными ИБ-решениями

Обеспечение процессов информационной безопасности — трудоемкий и ресурсозатратный процесс. Например, только содержание ИТ и ИБ сотрудников различных специализаций в штате может вылиться для компании в крупную сумму.

В случае аренды ИТ-инфраструктуры финансовые издержки на закупку оборудования, программного обеспечения, обучение и найм квалифицированного персонала не ложится невосполнимыми потерями на клиента. В случае IaaS не нужно ждать поставку оборудования — основные средства защиты уже находятся на площадке провайдера и предоставляются как сервис. Не нужно выбирать и кастомизировать ИБ-решение под себя — специалисты помогут выбрать необходимые компоненты защиты и обеспечат их бесперебойную работу и быстрый ввод в эксплуатацию. Таким образом, запуск ИБ-проектов проходит гораздо быстрее.

Если компания еще не имеет собственного департамента безопасности со штатом сертифицированных специалистов, вопрос защиты информационной системы логичнее доверить подрядчику, имеющему многолетний и многогранный опыт интеграции решений по защите информации с различными видами инфраструктуры и готовому предоставить инфраструктуру под конкретный запрос. Все, что требуется — обратить внимание на наличие у компании необходимых компетенций, опыта, примеров кейсов внедрения, лицензий, сертификатов и необходимых вычислительных мощностей для организации нужной инфраструктуры.

Услуги Selectel в сфере ИБ

О Selectel

Selectel – надежный провайдер IT-инфраструктуры в России. За свою 11-летнюю историю Selectel заслужил доверие более 15 тысяч клиентов – от индивидуальных предпринимателей до крупных международных корпораций.



Selectel предоставляет широкую линейку инфраструктурных продуктов и услуг, как собственной разработки, так и в партнерстве с мировыми технологическими лидерами:

- услуги дата-центров,
- выделенные серверы любых конфигураций,
- облачные сервисы на базе OpenStack,
- облако на базе VMware,
- облачные продукты AWS, Microsoft, Google, Alibaba Cloud,
- сетевые услуги, сеть доставки контента (CDN),
- защищенный сегмент ЦОД и услуги защиты информации,
- услуги по управлению IT-инфраструктурой (managed services),
- услуги консалтинга и интеграции.

Наша сеть насчитывает 6 современных дата-центров в Москве, Санкт-Петербурге и Ленинградской области.

Selectel предоставляет как комплексные, так и модульные услуги, что позволяет создать безопасную инфраструктуру, учитывая бизнес-потребности и особенности заказчика – от небольших компаний до транснациональных корпораций.

Инфраструктурные решения

Выделенные серверы в защищенном сегменте ЦОД

Это [услуга](#) для информационных систем с высокими требованиями к обеспечению защиты информации. Хранение и обработка персональных данных с выполнением требований № 152-ФЗ.

- Размещение в инфраструктуре защищенного сегмента дата-центра.
- Физическое отделение сети от других клиентов дата-центра.
- Дополнительные средства защиты в зависимости от защищаемой системы.

Дополнительные сервисы для защиты инфраструктуры

Для обеспечения доступности

- [построение отказоустойчивых сетей VRRP](#),
- [резервированное подключение MC-LAG](#),
- [подключение по протоколу BGP](#),
- [резервное копирование](#).

Для защиты инфраструктуры

- [аренда файервола](#),
- [средства WAF \(Web Application Firewall\)](#),
- [сервис защиты API](#),
- [линейка решений по защите от DDoS-атак](#).

Каждое решение может учитывать различные задачи клиента. Например, совместно с компаниями DDoS-Guard, Qrator и Incapsula, предоставляющими услуги защиты от DDoS-атак, мы предлагаем три варианта надежной защиты от DDoS-атак:

Решения Selectel для защиты от DDoS-атак / Технические характеристики	Базовая защита	Qrator	Incapsula
Индивидуальные настройки защиты (пользовательские правила)	✗	можно сделать по заявке	✓
Общее количество узлов фильтрации ¹	5	9	45
Количество узлов фильтрации в России ¹	1	2	1
Суммарная полоса фильтрации	1,2 Тбит/с	1,0 Тбит/с	6,0 Тбит/с
Защита от новых типов атак на основе интеллектуального модуля машинного обучения ²	✗	✓	✓
Доступность сайта в расчете на временной интервал соответственно соглашению об уровне обслуживания (далее SLA)	99,500%	от 97,000%	99,999%

¹ Атака «гасится» на ближайшем к источнику возникновения узле. Чем больше узлов у компании, тем эффективнее защита.

² Анализ произошедших у других клиентов атак. Чем больше атак проанализировано, тем шире база для обучения. Как следствие, аналогичные атаки «гасятся» намного быстрее.

Для защиты сетевого периметра

Сервисы могут предоставляться как в виде отдельного оборудования/программно-много обеспечения, так и в виде комплексной услуги с администрированием:

Название подсистемы ИБ	Предоставление доступа к средствам защиты информации
Межсетевое экранирование	Аренда межсетевого экрана Fortinet FortiGate 100D
Межсетевое экранирование	Аренда сертифицированного межсетевого экрана Fortinet FortiGate-100D-LENC
СОВ	IPS/IDS для FortiGate 100D

В рамках индивидуальных проектов дополнительно предоставляются:

- система обнаружения вторжений,
- VPN-соединения до удаленных точек и мобильных пользователей,
- антивирусная защита,
- защита от несанкционированного доступа,
- анализ защищенности инфраструктуры,
- администрирование средств защиты.

Почему Selectel

Selectel строго соблюдает как требования надзорных органов, так и следует актуальным методам защиты информации.

Соответствие требованиям законодательства РФ

Лицензии ФСТЭК и ФСБ для оказания услуг в области защиты информации. Защита персональных данных согласно 152-ФЗ. Хранение персональных данных согласно 242-ФЗ. Соблюдение требований для подключения к государственным ИС. Размещаем информационные системы персональных данных (ИСПДн) с IV по I (максимальный) уровень защищенности.

Сертификация PCI DSS

Selectel имеет сертификаты PCI DSS – стандарт безопасности данных индустрии платежных карт и ISO/IES 27001 – международный стандарт по информационной безопасности что подтверждает следование одним из самых требовательных стандартов безопасности.

Индивидуальный подход

Мы предлагаем широкую линейку сервисов для защиты информации. Проявляя заботу о защите персональных данных ваших клиентов, вы повышаете ценность вашего бизнеса.

Оперативность

Не нужно ждать поставок оборудования, основные средства защиты уже находятся в наших дата-центрах и предоставляются как сервис.

Надежная защита

Богатая экспертиза по построению защищенных сетей в дата-центрах Selectel для

обеспечения защиты коммерческой тайны. Физическая безопасность. Контроль доступа, дополнительный периметр безопасности. Сетевая безопасность. Защищенная изолированная сеть на основе защищенного сегмента ЦОД.

Гибкость

Selectel обеспечивает высокие показатели отказоустойчивости и масштабируемости инфраструктуры, которые по ряду причин невозможно развернуть в собственной инфраструктуре.

Топ-1

наиболее динамичная компания рынка IaaS в России¹

Топ-2

провайдер частных облаков в России²

Топ-1

компания в номинации «Технологии и инновации»³

Топ-4

игрок в сегменте colocation⁴

Топ-2

самый зрелый провайдер облачных услуг в России⁵

Топ-5

IaaS-провайдер в России¹

¹ Источник: iKS-Consulting ranking.

² Источник: IDC ranking.

³ Источник: «Премия Рунета» 2018.

⁴ Источник: iKS research.

⁵ Источник: TAdviser ranking.

Примеры кейсов

Платежный сервис

Задача: безопасно обрабатывать финансовые данные, выполнить дополнительные требования СТО Банка России, соответствовать стандарту PCI DSS, минимизировать ИБ-угрозы.

Решение: клиент использует услуги Selectel для хранения и обработки конфиденциальных данных. Для нейтрализации угроз безопасности клиент подключил услуги по защите web-приложений и защиту от DDoS-атак.

Результат: клиент успешно прошел сертификацию на соответствие требованиям PCI DSS.

Медицинская лаборатория

Задача: безопасно хранить и обрабатывать медицинские базы данных и биометрические сведения, обеспечить защиту данных от внешних атак.

Решение: на выделенном сервере в защищенном сегменте дата-центра Selectel клиент размещает персональные и биометрические данные клиентов. Для нейтрализации рисков, связанных с утечкой корпоративных данных, клиент использует шифрование каналов связи, антивирусную защиту для ПК и серверов.

Результат: удалось минимизировать информационные угрозы и повысить доступность IT-инфраструктуры.

Туристический оператор

Задача: построить защищенную систему общего доступа к файловому хранилищу для клиентов, партнеров и подрядчиков. Безопасно обрабатывать паспортные и прочие данные туристов.

Решение: компания использует услуги Selectel для хранения и обработки персональных данных своих клиентов. Для повышения безопасности дополнительно были подключены сервисы сетевого антивируса и сетевой песочницы.

Результат: построив безопасную IT-инфраструктуру, компания выполнила требования корпоративных стандартов по защите информации и предоставила доступ к необходимым данным для клиентов и подрядчиков в режиме онлайн.

Постройте защищенные информационные системы с Selectel

Наши специалисты подберут оптимальный вариант защиты, учитывая специфику приложения, факторы риска и уровень угроз — как по предварительным данным, так и учитывая растущий ландшафт и уровень угроз.

В зависимости от сложности инфраструктуры/веб-приложения, особенностей и предназначения могут быть использованы от базовых средств защиты до глобальных сетей доставки контента (CDN) для борьбы с DDoS, очистки от нелегитимного трафика, кэширования и доставки приложений к пользователю, балансировки нагрузки веб-сервисов.

Благодаря комплексному подходу к защите информационных систем, вы получите всестороннее решение, иначе доступное на рынке лишь в виде компонентов от различных поставщиков.

[Запросить коммерческое предложение](#)

Selectel

123060, Россия, г. Москва,
улица Берзарина, д. 36, стр. 3
Телефон: +7 495 647 79 80

196084, Россия, г. Санкт-Петербург,
улица Цветочная, д. 21, лит. А
Телефон: +7 812 677 80 36

www.selectel.ru