Финансист

FREEDOM finance

Журнал о личных инвестициях, брендах и акциях

№1(01)2019

ФИНТЕХЗАЩИТА

Вся вашингтонская рать

Оборона заказа

От автокресла до автопилота

Доходные отходы

FREEDOM finance

АО «Фридом Финанс». Лицензия на осуществление деятельности на рынке ценных бумаг №3.2.238/15 от 02 октября 2018 года. www.almaty-ffin.kz. Реклама.

bonds.kz

7555

Стирая грань между реальным и виртуальным

ТИМУР ТУРЛОВ,
генеральный директор ИК «Фридом Финанс»

В июне 2016 года основатель социальной сети Facebook Марк Цукерберг опубликовал в Instagram свое фото на рабочем месте с подписью о том, как он рад росту аудитории сервиса. «Это все благодаря Кевину Систому и Майку Кригеру [основатели Instagram] и всем тем, кто открыл окно в свой мир, делясь крупными событиями или моментами из повседневной жизни», — заключил Цукерберг.

Этот пост остался бы без внимания мировой общественности, если бы не одна интересная деталь: на фотографии видно, что веб-камера и микрофон на рабочем ноутбуке героя заклеены изолентой.

О том, насколько важна безопасность личных данных, глава компании с миллиардами клиентов и терабайтами конфиденциальной информации знает не понаслышке. Через несколько лет ему придется публично оправдываться за утечку информации о десятках миллионов пользователей Facebook в стороннюю компанию и пересмотреть политику конфиденциальности.

Мы живем в мире, где обеспечивать безопасность и сохранность личной жизни, объекта или информации становится все сложнее. И дело не только в хакерах и киберпреступниках — утечки могут происходить совершенно случайно и без злого умысла.

Конечно, в таких условиях растет спрос на услуги компаний, работающих в сфере безопасности. Одни торгуются на бирже и приносят своим инвесторам хороший доход, другие, например Palantir, уже давно находятся в поле зрения Уолл-стрит. Их IPO наверняка станет знаковым событием для биржевого мира.

В этом номере «Финансиста» мы рассказываем о компаниях, обеспечивающих безопасность в широком смысле. К этой сфере относятся производители военной техники, разработчики систем кибезащиты и даже переработчики отходов. Ведущие аналитики и эксперты рассказывают о том, в каком направлении развивается отрасль и как на этих изменениях можно заработать.

Приятного чтения!

Журнал «Финансист» №1 (01) 2019
Собственник: ТОО «Alteco Partners». **Главный редактор:** Марат Каирбеков. **Выпускающий редактор:** Наталья Харлашина. **Дизайн, инфографика:** Филипп Косарев, Станислав Вербель. **Корректор:** Татьяна Нарышкина. **Координаторы выпуска:** Рамина Фахрутдинова. **Фото в номер:** shutterstock.com. **Иллюстрация на обложке:** Маргарита Миргазова. Журнал зарегистрирован в Министерстве информации и коммуникаций РК. Свидетельство о постановки на учет №.17775-Ж от 03.07.2019 г.
Адрес редакции: A15E3B3, Республика Казахстан, г. Алматы, пр. Аль -Фараби, д. 7, Бизнес-центр «Нурлы Тау», блок 5А, оф. 119, Тел.: + 7 (727) 346 84 41. E-mail: info@ffin.kz. Подписано в печать: 23.09.2019. Тираж: 5 500 экз. Журнал распространяется бесплатно. **Отпечатано:** Типография «Sprinter», 050031, Республика Казахстан, г. Алматы, ул. Утеген батыра, д.7/2, тел: +7 (747) 094 36 14, e-mail: info@sprinter.kz, сайт: www.sprinter.kz

Вся вашингтонская рать

Как американские компании зарабатывают на тяге к войне

Вадим Меркулов,
директор
аналитического департамента
ИК «Фридом Финанс»

Расходы на оборону являются одной из ключевых статей бюджета любого государства, особенно Соединенных Штатов. И хотя публичные компании, обслуживающие этот сектор экономики, уступают по доходности технологическому и биотехнологическому секторам, их продукция будет востребована всегда.

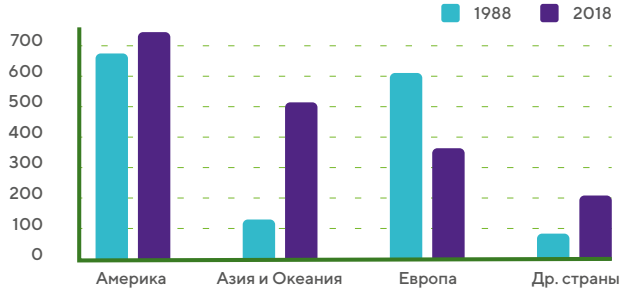
Гонка вооружений

В 2018 году мировые затраты на оборонный сектор выросли до рекордных с момента окончания холодной войны $1,822 трлн, что составило 2,1% глобального ВВП. За 30 лет относительный прирост составил 18,8%, причем основной вклад в общую динамику внесли страны Азии и Океании, чьи военные расходы росли ежегодно и в общем прибавили 267,8%.

В Европе во время холодной войны сектор расширялся в основном за счет Советского Союза, после распада которого и до сегодняшнего дня затраты на оборонный сектор в регионе упали более чем на 40%.

В 2018 году мировым лидером по расходам на оборону

Затраты на оборонный сектор, $ млрд

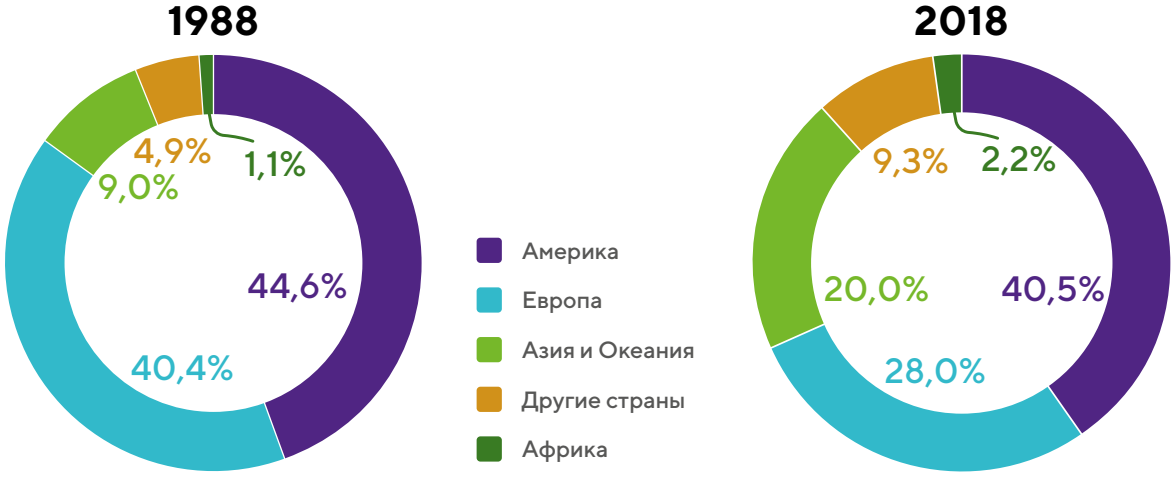


Источник: данные SIPRI

по-прежнему остаются США. Сумма их военных расходов в абсолютном выражении превысила $648 млрд, впервые с 2010 года увеличившись на 4,6% и составив 36% от общемирового показателя.

В 1989 году доля США была 50%. Тогда в топ-5 (исключая США) входили Франция, Германия, Великобритания, Япония и Италия. Сегодня в этом рейтинге — Китай, Саудовская Аравия, Индия, Франция и Россия.

Доля стран в общемировых затратах на оборонный сектор



Источник: данные SIPRI

К слову, Поднебесная демонстрирует прирост расходов уже 24-й год подряд. По мнению специалистов Стокгольмского института исследования проблем мира (SIPRI), в 2018 году половина мировых расходов на оборонный сектор пришлась именно на Китай и Америку.

В основном военная отрасль финансируется государством. Например, в Белоруссии затраты госбюджета на оборону превышают 30%. В России и США этот показатель находится в пределах 10%, в европейских странах от 1 до 5%, и 5,5% — в Китае.

Помимо того что США лидируют по объемам затрат на военный сектор, они также остаются крупнейшим производителем и экспортером вооружения. В топ-100 крупнейших военно-промышленных компаний входят 42 предприятия из США — на их долю приходится 57% от общего объема продаж. На втором месте Россия с 9,5%.

Агрессивные янки

Несмотря на огромный бюджет американской армии и ВПК, сейчас военный сектор США вряд ли можно назвать перспективным. Расходы на оборону в Штатах расти не будут, потому что и так находятся на локальных максимумах. После очередного увеличения потолка госдолга наращивание военных расходов не получит одобрения в Конгрессе.

Сохранится финансирование ряда ключевых программ: разработка бомбардировщика B-2 (производится компанией Northrop Grumman Corp.; тикер NOC), самолета-заправщика KC-46 (Boeing; BA), истребителя F-35 (Lockheed Martin; LMT), нескольких субмарин и «дестроеров» (General Dynamic; GD). Заказы на эти программы поддержат выручку компаний, но ситуация кардинально не улучшится, а значит и котировки их акций будут находиться под давлением.

С другой стороны, рост геополитической нестабильности, популизма и деглобализации повышает вероятность военных конфликтов. Сейчас наиболее актуальный сценарий — это столкновение США с Ираном, несмотря на заявления политиков с обеих сторон об обратном.

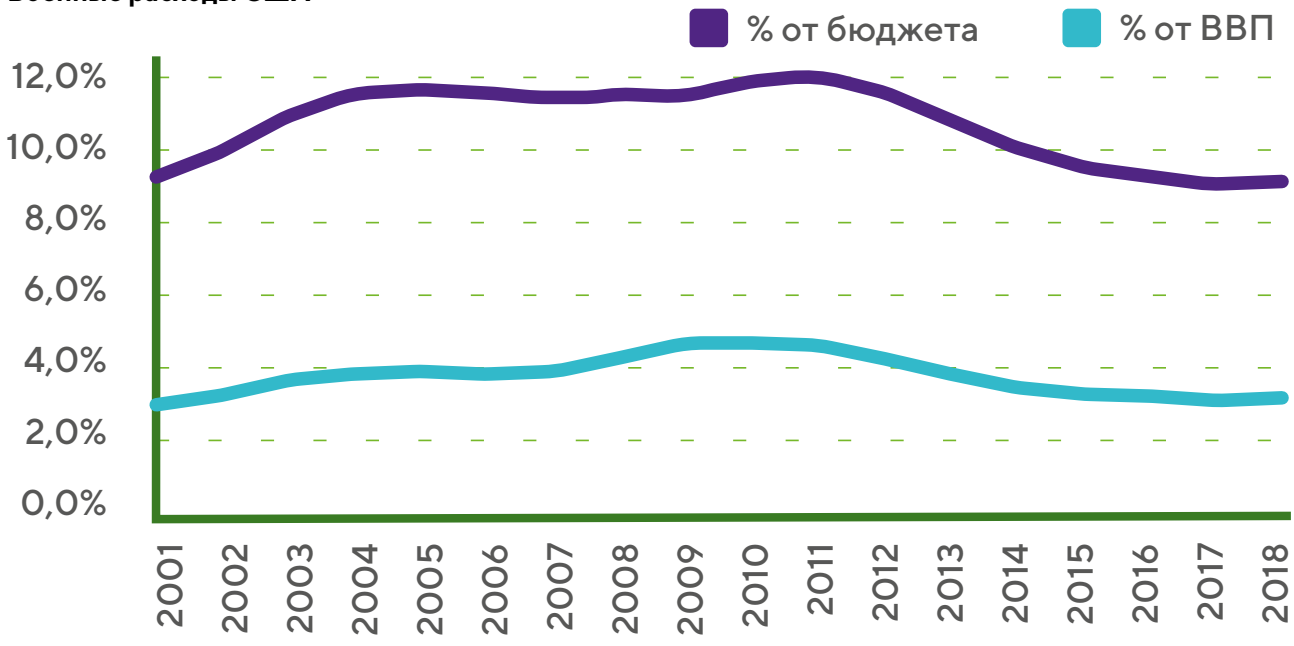
Открытое противостояние вызовет краткосрочный рост «военных» котировок, а основным долгосрочным драйвером является военный бюджет США, который, тем не менее, не будет активно расти. Ожидаем, что затраты на оборону США в 2020-м приблизятся к $650 млрд, прибавив порядка $1 млрд, или 0,3%.

Фундаментальные причины говорят о слабом драйвере для военных компаний, но лучше рассмотреть каждую из них подробнее для поиска самых перспективных бумаг сектора.

United Technologies (UTX). Выручка компании поступает из четырех сегментов бизнеса: Otis — производство лифтов, Carrier — производство холодильников и кондиционеров, Pratt & Whitney — производство двигателей для пассажирских и военных самолетов, и Collins Aerospace — разработка военных истребителей и ракет.

Для повышения эффективности бизнеса компания планирует разделиться на три самостоятельные фирмы к началу 2020 года. Otis и Carrier выделятся в отдельные публичные компании, а оборонный сегмент в лице Pratt & Whitney и Collins Aerospace окажется

Военные расходы США



Источник: данные SIPRI

в одной структуре. Соответственно, компания станет практически полностью военной уже спустя год.

В текущем году ожидается прирост выручки United Technologies на 16%. Долговая нагрузка высока при низких показателях ликвидности, что типично для крупных игроков рынка оборонной промышленности США. Коэффициент покрытия процентных платежей составляет 4,5, что ниже медианного значения за три последних года в 9,4. Мультипликаторы компании EV/Revenue и EV/EBITDA находятся выше медианных по индустрии, как и P/E, равный 20,07. Целевая цена по компании — $142 до конца второго квартала 2020 года.

Lockheed Martin (LMT). Компания работает по четырем направлениям: Aeronautics, Missiles and Fire Control, Rotary and Mission Systems и Space. Сегмент Aeronautics занимается разработкой боевых истребителей, вертолетов и прочей авиатехники. Самый известный продукт — тот самый F-35, который пользуется у Пентагона особой популярностью.

Missiles and Fire Control разрабатывает тактические ракеты, системы наведения для военных вертолетов марки «Апач» и многое другое. Rotary and Mission Systems производит ракетные установки для военных судов, беспилотные дроны, радарные установки для обнаружения противников и сонары. Наконец, сегмент Space занимается разработками спутниковых систем, систем наземной связи и ракет стратегического назначения.

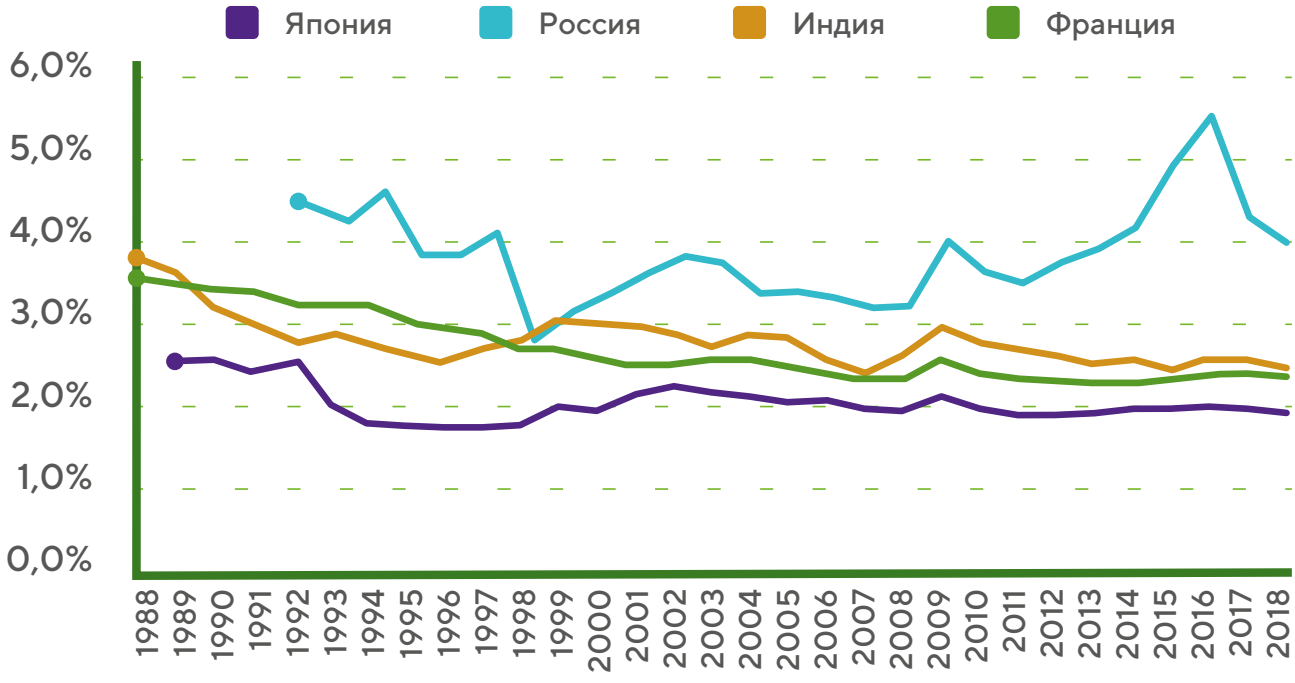
В этом году выручка компании может подняться на 7,7%. Также растет на 11% и операционная эффективность на фоне оптимизации производства F-35, который приносит 25-30% от выручки. Коэффициент P/E находится на уровне 18,07, что выше медианного по индустрии в 17,22, но благодаря улучшению своей маржинальности Lockheed Martin может достигнуть 19-20 пунктов уже в 2020 году.

Boeing (BA). Выручка компании приходится на сегменты Commercial, Defense, Space и Services. В первом, коммерческом, сегменте компания разрабатывает гражданские пассажирские самолеты. Оборонный дивизион производит военные истребители, радары для систем ПВО, беспилотные самолеты, продукты кибербезопасности и ракетные системы. Якорный продукт — самолет-заправщик KC-46, о котором мы уже упоминали.

В космическом сегменте компания ведет разработки спутников, тренажеров для астронавтов и военных систем связи на земле. Сервисное подразделение разрабатывает программное обеспечение для управления полетами, собирает и анализирует данные.

Выручка Boeing в 2019 году упадет на 8,4% из-за крушения двух авиалайнеров модели 737 MAX в связи

Военные расходы, % от ВВП



Источник: данные SIPRI

с ошибками в программном обеспечении самолетов. Ключевой вопрос для инвесторов: сможет ли компания возобновить производство 737 MAX, на который возлагались большие надежды? Так что финансовые показатели отходят на второй план, поскольку находятся в рамках индустриальных значений. Если регулятор разрешит возобновить полеты нового авиалайнера, акции компании могут вернуться к своим историческим максимумам.

Northrop Grumman Corp. (NOC). Это полностью военная компания, выручка которой формируется четырьмя сегментами: Aerospace Systems, Innovation Systems, Mission Systems и Technology Services. В сегменте Aerospace Systems компания занимается разработками военных морских кораблей, воздушных истребителей и прочей техники. Innovation Systems разрабатывают ракеты моделей Super Hornet и Growler, которые поставляются для истребителей F-35 и Военно-морских сил США.

Mission Systems производит радары марки MESA, системы ПВО, запуска баллистических ракет и многое другое. Technology Services готовит программное обеспечение для военных.

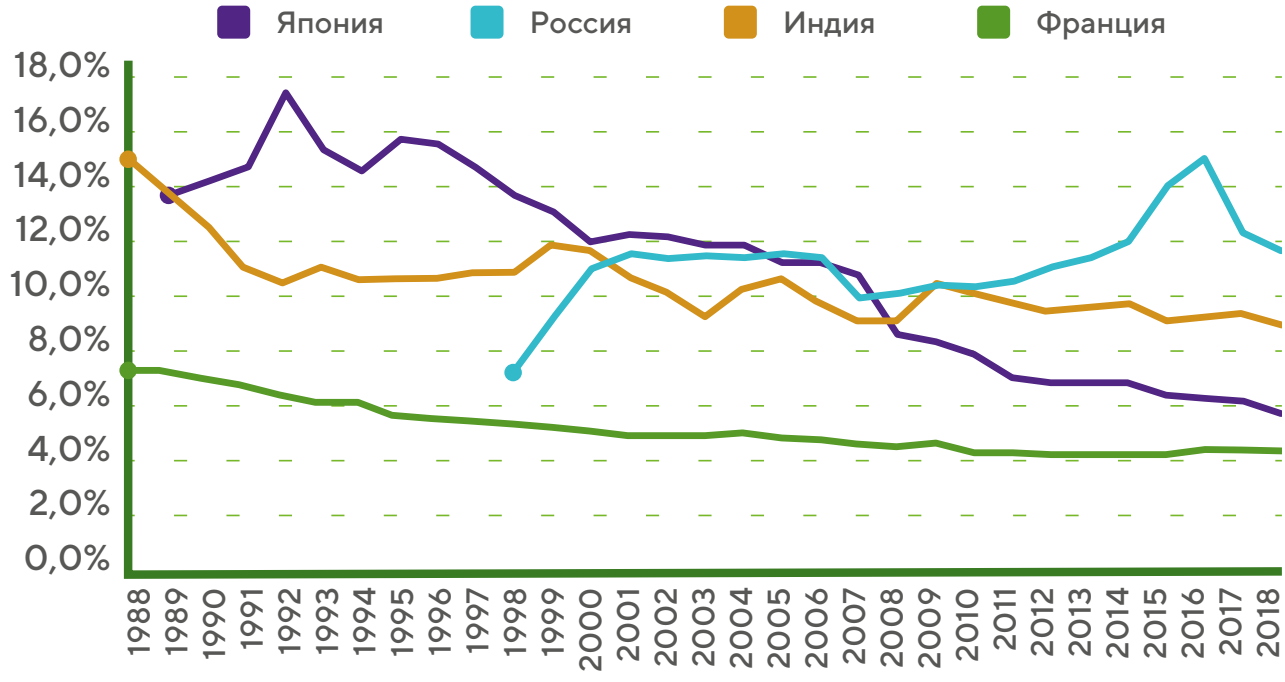
В текущем году выручка Northrop Grumman Corp. вырастет на 10,5%. Коэффициент покрытия процентных платежей составляет 6,8, что ниже медианного в 9,4. Показатель Чистый долг/EBITDA равен 3,1, что выше медианного показателя в 2,15. Мультипликаторы компании EV/Revenue и EV/EBITDA находятся выше средних по индустрии. P/E при этом торгуется ниже медианы индустрии, на уровне 16,37.

General Dynamic (GD). Компания выпускает двигатели для пассажирских самолетов и самолеты марки Gulfstream, а также наземные боевые системы для пехотных войск (танки «Абрамс»), военные крейсеры и лодки для ВМС, центры связи для военных операций, радары для обнаружения противника и т. д.

В текущем году General Dynamic может заработать на 6,9% больше, чем в 2018-м. Долговая нагрузка компании высока, коэффициент покрытия процентных платежей составляет 8,7, что ниже медианного в 9,4. Чистый долг к EBITDA равен 2,7, что выше среднерыночного показателя в 2,15. Мультипликаторы компании EV/Revenue и EV/EBITDA находятся ниже, чем по индустрии, так же как и P/E.

В целом наиболее перспективными компаниями являются Lockheed Martin и United Technologies. Первая остается крупнейшим в мире производителем вооружений с объемом продаж в $45 млрд. Благодаря смене оргструктуры United Technologies сможет сфокусироваться на военном секторе, что также позитивно скажется на капитализации бизнеса.

Военные расходы, % от бюджета



Источник: данные SIPRI

Оборона заказа

Почему так сложно частному инвестору вложиться в российскую армию

Георгий Ващенко,
начальник управления операций на российском фондовом рынке ИК «Фридом Финанс»

Россия занимает второе место в мире по объему экспорта вооружений, уступая только США. Доля отечественных производителей на мировом рынке — 21%.

В 2018 году экспорт российской военной техники побил рекорд и составил $13,7 млрд. Портфель международных заказов «Рособоронэкспорта» сейчас оценивается в $55 млрд, и это тоже рекордный показатель. Прибыль предприятий холдинга «Ростехнологии», которые производят оборонную продукцию, достигла 128 млрд рублей. Если сравнивать лишь с американской корпорацией Lockheed Martin, которая зарабатывает в год $5,5 млрд, — немного.

Но даже этой небольшой прибылью государство, как основной акционер «оборонки», делиться не будет. И вот почему.

Хотя в России работают сотни выпускающих военную продукцию предприятий и часть из них имеет статус публичных акционерных обществ (ПАО), их бумаги непросто купить или продать: ликвидность бумаг низкая, частные инвестиции обходят сектор стороной, миноритарных акционеров почти не осталось.

Антироссийские санкции больно ударили по оборонной сфере, так как мешают компаниям выйти на мировой рынок. Некоторым из них удалось выжить на фондовом рынке, однако пришлось сильно сократить корпоративную открытость. Например, ОАК в 2019 году не опубликовала ни одной презентации для инвесторов и отчетности за прошлый год. «Звезда» вообще перестала выкладывать любую информацию. Публичные акционерные общества по факту стали закрытыми.

Их осталось трое, а точнее — один

Сейчас в списке торгуемых бумаг на Московской бирже остались акции лишь нескольких компаний, выпускающих военную продукцию: помимо упомянутой «Звезды», это «КАМАЗ» и «Объединенная авиастроительная корпорация» (ОАК), а также ее дочерняя корпорация «Иркут». Государство контролирует более 90% ОАК, которая, в свою очередь, контролирует 95% «Иркута».

ОАК представляет интерес для инвесторов как производитель авиатехники в целом. Но пока объем военных заказов преобладает.

Портфолио ОАК включает в себя 7 гражданских и многоцелевых самолетов, 9 типов боевых машин и 3 типа для военно-технической авиации. Но большинство гражданских самолетов находится в стадии проектирования или мелкосерийного производства. Почти весь объем производства приходится на одну модель — пассажирский самолет SSJ-100.

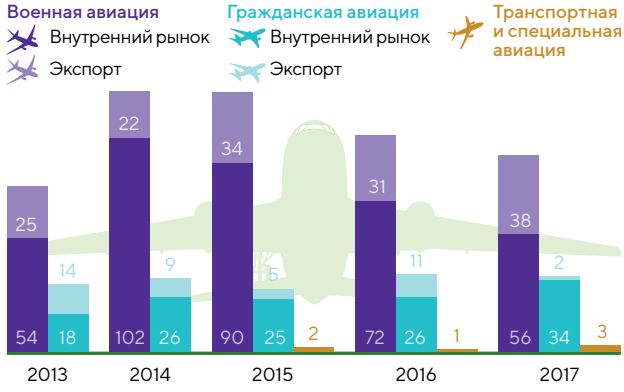
Ситуация будет меняться медленно. Рынок заказов на региональные реактивные самолеты в сегменте SSJ-100 компания оценивает в $190 млрд. Емкость сегмента узкофюзеляжных самолетов, к которому относится МС-21, — $3,4 трлн. В России, основном рынке для самолетов ОАК, сейчас дефицит техники.

Заказано более 400 единиц SSJ-100, произведено и отгружено покупателям 190 единиц. Еще почти на 80 машин есть опцион. Но объем производства невозможно нарастить из-за ограниченных мощностей поставщика двигателей, компоненты которого изготавливаются во Франции. Санкции и прочие проблемы с импортом, требующие увеличения степени локализации комплектующих, также задерживают серийное производство МС-21 — оно начнется в 2020-2021 году.

Капитализация ОАК сегодня около $5,5 млрд, «Иркута» — $750 млн. Низкая стоимость бизнеса обусловлена несколькими факторами: небольшое число акций в обращении, финансовая непрозрачность, отсутствие дивидендов последние три года, сложности с производством и его расширением из-за нехватки денег и так далее.

Неудивительно, что на этом фоне инвесторы проявляют куда больший интерес к бумагам американских оборонных компаний, чем к родному ВПК.

Динамика поставок воздушных судов, шт.



Источник: Годовой отчет ОАК

«В Даркнете узнают об утечке информации раньше, чем ее может обнаружить компания»

Создатель и CTO компании Locus Soft Technologies Алексей Авраменко — о том, как она помогает клиентам следить за их данными в «темной» части интернета

О DeepHound (проекте Locus Soft Tech) нет информации в открытом доступе. Как о вас узнают потенциальные клиенты?
В основном это сарафанное радио и контакты, собранные за 17 лет работы в области защиты информации. Наша команда позиционирует себя как эксперт в области информационной безопасности

Алексей Авраменко, создатель и CTO компании Locus Soft Technologies

на территории России и в некоторых международных проектах. На данный момент мы рассматриваем возможность глобального выхода на зарубежные рынки.

Расскажите, пожалуйста, о ваших проектах.
У нас два бизнеса. Первый — это компания, занимающаяся стандартной защитой конфиденциальных данных: оказывает услуги по защите информации, аудиту, консалтингу, аттестации объектов информатизации, проводит комплексное тестирование на проникновение во внутренние и внешние сети, веб-ориентированные информационные системы, интранет и мобильные приложения (iOS, Android) по российским и международным стандартам и мировым Best Practice.
Второй — компания Locus Soft Technologies (далее LST). Она занимается разработкой и продвижением новых перспективных технологий и продуктов. LST занимается сервисом DeepHound, интеллектуальной IT-платформой для мониторинга и выявления критических угроз как в открытом, так и в закрытом интернете.

Источниками утечек данных являются сотрудники, из-за этого компании теряют деньги. Возможно ли с помощью разрабатываемых вами инструментов устранить человеческий фактор?
Мы можем помочь уменьшить риски, связанные с этим фактором. В Даркнете, например, можно узнать об утечке данных намного раньше, чем она будет зафиксирована самой организацией. У нас был случай, когда чувствительная информация компании, добытая путем взлома их внутренних ресурсов, продавалась на одной из площадок Даркнета. Обнаружив это, мы оперативно сработали и уведомили ее об этом.

Можно ли оценить экономический эффект от предотвращения утечки? И какие санкции применяет компания к проштрафившимся сотрудникам?
Конкретные кейсы мы не имеем права обсуждать из-за подписанных нами документов о неразглашении, к тому же каждый такой случай субъективен. Могу лишь сказать, что в России потенциальные экономические потери небольшие — разве что страдает репутация компании. Конечно, допустившим утечку сотрудникам потом сложно устроиться на нормальную работу.
За рубежом другая ситуация. Если ваши данные утекли, вы можете подать в суд серьезный иск на компанию и выиграть дело. Поэтому в условиях жесточайшей конкуренции банки и финансовые организации следят за своей репутацией и стараются более серьезно подходить к минимизации рисков, так как могут быть значительные финансовые потери.

Чем российский клиент отличается от иностранного?
Работать с зарубежными клиентами часто удобнее, чем с российскими, так как они более позитивно относятся к инновациям. И даже если их что-то не устраивает в продукте, они обычно просят нас доделать или переделать не устраивающий их функционал. То есть проявляют открытость и гибкость.
Службы безопасности в некоторых российских финансовых организациях смотрят искоса на наш сервис DeepHound, в том числе потому, что он в некоторых аспектах заменяет их должностные обязанности.

Кто еще является вашим клиентом?
Это компании, которые активно работают с другими компаниями, то есть B2B-сектор.

Как изменились ваши доходы за последние два года?
Мы растем на 25% каждый год.

Сколько стоят ваши услуги?
Стоимость заказа составляет в среднем $120 тысяч, в целом ценовую политику мы формируем в соответствии со стратегией «ценовой дискриминации».

Повлияли ли на вашу работу антироссийские санкции, закон «О суверенном интернете» или «закон Яровой»?
Эти законы не влияют, а вот санкции дают о себе знать. Они являются одной из причин, почему мы не могли до сих пор выйти на зарубежный рынок. В мире смотрят на любой российский бизнес с большой осторожностью. Зарубежные инвесторы часто не готовы инвестировать в российскую компанию.

Согласуете ли вы свою работу с силовыми структурами?
На данный момент мы не работаем с силовыми структурами. Наша задача — собрать информацию под заказчика и передать ее, а дальше выводы делает он сам. Мы не лезем во внутренние системы клиента, у нашего продукта «внешний» алгоритм. Поэтому не требуется согласования каких-то дополнительных структур.

Какие новые секторы экономики вам интересны?
Сейчас активно развивается индустрия интернета вещей, и там тоже есть свои особенности в плане обеспечения информационной безопасности. Условно говоря, теперь злоумышленник может не только узнать информацию о вашем «умном» холодильнике, но и разморозить его *(смеется)*.
А если серьезно, то интернет вещей представляет собой отдельную сеть, связанную с интернетом. И чтобы с ней работать, нужно использовать дополнительные программы для анализа данных. Это первое. А второе — предотвращать возможность использования этих сетей, например, для совершения DDoS-атак с последующим выводом из строя подключенного к ним оборудования, а также получения чувствительной информации о пользователях этого оборудования.
Над решением этих проблем мы также активно работаем.


Источник: shutterstock.com

Кибердоход

Самый простой способ вложиться в отрасль кибербезопасности — купить акции биржевого инвестиционного фонда ETFMG Prime Cyber Security ETF. Разберем его сильные и слабые стороны с позиции частного инвестора

Ален Сабитов,
аналитик
ИК «Фридом Финанс»

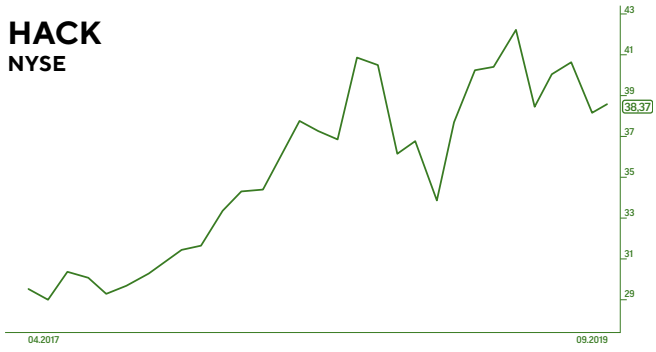


График котировок ETFMG Prime Cyber Security ETF

ETFMG Prime Cyber Security ETF (тикер HACK) появился в 2014 году. По сути это корзина из акций компаний, которые работают в индустрии кибербезопасности. Покупая бумаги фонда, инвесторы тем самым получают доступ к перспективному сектору.

К сожалению, HACK имеет недостатки: его акции низколиквидны. Это значит, что по ним проходит очень небольшой объем торгов и они пока не пользуются популярностью у массового инвестора. То есть для тех, кто захочет вложить больше $3 млн, будет достаточно сложно это сделать без косвенного убытка в 0,1-0,2% .

Это объясняется тем, что кибербезопасность — это узкоспециализированный сектор, который пока не занимает значительного места на американском фондовом рынке.

Теперь о сильной стороне фонда — о его составе. В ETF входит 37 компаний, каждая из которых является перспективным игроком в секторе кибербезопасности, облачной защиты и защиты IT-инфраструктуры. Мы выделили трех самых многообещающих игроков на отрезке 10 лет.

Symantec Corp (тикер SYMC)

Компания разрабатывает программы и сервисы для защиты информации и конфиденциальности данных. Базируется в Кремниевой долине, появилась в 1982 году, а через 7 лет разместилась на бирже NASDAQ. Акции Symantec Corp входят в расчет индекса S&P 500, капитализация компании составляет $12,9 млрд.

Одно из ключевых направлений деятельности — разработка сервисов защиты сегмента интернета вещей (IoT), который активно развивается в последние годы. Это миллиарды связанных между собой «умных» устройств в здравоохранении, информационных технологиях, телекоммуникациях, банковском деле, финансовых услугах, страховании, автомобильной промышленности и др. Они собирают и обмениваются данными без участия человека.

Сегодня количество IoT-устройств в мире насчитывает от 7 до 10 млрд. Сколько еще к ним присоединится через два года — никто толком не знает. Gartner, одна из крупнейших исследовательских компаний, прогнозирует 25 миллиардов к 2021 году, а Intel и вовсе говорит о 200 миллиардах.

К большинству таких устройств можно будет подключиться удаленно, и обход защиты открывает доступ ко всей Сети и гигантским массивам данных. Symantec входит в число мировых лидеров по IoT-безопасности

Symantec. Генштаб. Источник: shutterstock.com

График котировок Symantec Corp

наряду с такими крупными игроками, как IBM, Cisco, Intel, Kaspersky Lab.

MobileIron Inc (MOBL)

Компания специализируется на безопасности мобильных устройств, приложений и облачных сервисов, включая управление мобильностью предприятия (EMM) и управление мобильными устройствами (MDM).

MobileIron разместилась на NASDAQ в 2014 году, рыночная капитализация находится в районе $750 млн. В 2009-2013 годах компания считалась самой быстрорастущей технологической фирмой в мире по оценке Deloitte.

В этом году MobileIron делает ставку на свой сервис mobile-centric zero trust security platform и опцию zero sign-on (стала доступна в июне 2019 года).

Первое новшество позволяет проверить мобильное устройство, а также обнаруживает и устраняет угрозы перед предоставлением безопасного доступа к внутренней сети.

Zero sign-on предполагает полное отсутствие логинов и паролей и аутентификацию по ID устройства. У нее два преимущества. Во-первых, пароли представляют угрозу безопасности, поскольку их легко взломать, а повторное использование может привести к целой волне взломов. Во-вторых, запросы на сброс паролей приводят к значительным затратам на поддержку системы.

По данным IDG (International Data Group), 86% руководителей, принимающих решения по безопасности компании, по возможности отказались бы от использования паролей, что означает потенциальный интерес к продуктам MobileIron и миллиардные выручки.

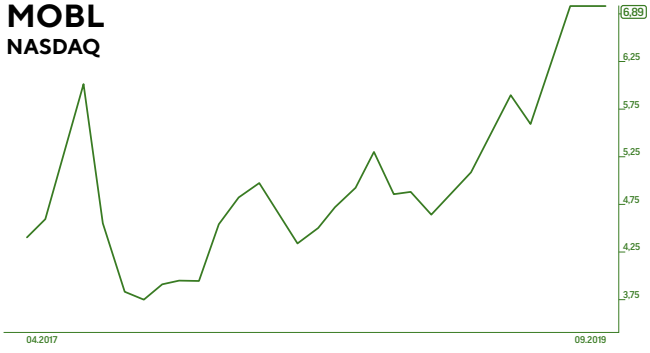


График котировок MobileIron Inc

OneSpan Inc (OSPN)

Компания, базирующаяся в Чикаго, предлагает облачную и открытую платформу для защиты от мошенничества. OneSpan внедряет клиентам мультифакторную аутентификацию и цифровые подписи для приложений, работающих на ПК, ноутбуках, планшетах и смартфонах.

Наиболее перспективным направлением для OneSpan является адаптивная мультифакторная аутентификация, которая становится особенно популярна в современной финансовой индустрии. Одной из ее опций является так называемая поведенческая биометрия, которая рассматривается не в качестве замены другим видам аутентификации, а как надстройка еще одного уровня безопасности. Она собирает и анализирует элементы поведения, включая силу давления пальца, скорость печатания и другие, и сравнивает их с данными в профиле пользователя. Качество аутентификации возрастает без ущерба для удобства.

Согласно докладу OneSpan, 60% опрошенных финансовых посредников планируют инвестировать в современную мультифакторную идентификацию. Рынок этой услуги будет расти в среднем на 18% в год в ближайшие 5 лет и к 2024 году может достигнуть $17 млрд. Рыночная капитализация OneSpan на NASDAQ составляет порядка $700 млн.

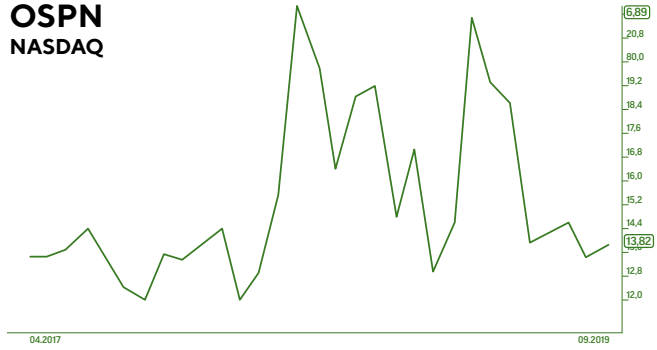


График котировок OneSpan Inc

Купить безопасность

ETFMG Prime Cyber Security ETF предоставляет доступ к высокотехнологическому будущему, которое сейчас пока еще сложно понять. Примерно такой же эффект имели облачные технологии 10-15 лет назад, а теперь облачный рынок — один из самых крупных и перспективных в технологическом секторе. Аналогичная судьба ждет и кибербезопасность, о чем говорит как минимум динамика стоимости ETF с момента начала торгов 5 лет назад — он подорожал на 50%.

Биржа ждет

Самые ожидаемые IPO в секторе кибербезопасности

Андрей Волощенко,
заместитель директора
департамента по работе с клиентами
ИК «Фридом Финанс»

Рынок первичных размещений сейчас на пике своей активности. Это можно легко понять по интересу инвесторов к уже вышедшим на биржу стартапам. Например, таким как Beyond Meat, Zoom, PagerDuty, ShockWave Medical и CrowdStrike Holding.

Акции этих компаний показали колоссальный рост. К 1 июля 2019 года с момента их первичных размещений прошло менее четырех месяцев, а средняя доходность по бумагам уже составила 210%.

Но Уолл-стрит жаждет новых имен, благо в мире есть много частных компаний из сегмента кибербезопасности, способных заинтересовать инвесторов своими акциями. Проведем краткую перекличку.

Palantir Technologies

Компания была создана в 2004 году группой инвесторов во главе с одним из основателей PayPal Питером Тилем, и сейчас она считается одним из самых влиятельных и дорогих стартапов, объем инвестиций в который составил более $2 млрд. Palantir занимается разработкой программного обеспечения и алгоритмов для сбора, обработки, анализа и защиты данных в сфере финансов, государственной безопасности, разведки и обороны.

Компания не стремится на биржу. В октябре 2018-го Palantir уже обсуждала возможность IPO при первоначальной оценке в $41-80 млрд, но размещения не произошло. Сейчас Уолл-стрит ожидает увидеть Palantir на бирже не раньше 2020 года, но никаких гарантий нет, поскольку компания тесно сотрудничает с Пентагоном. Контракты с военными очень прибыльны, и Palantir незачем привлекать дополнительные деньги.

Cloudflare

Фирма занимается предотвращением хакерских DDoS-атак и оптимизирует доставку данных с помощью глобальной сети прокси-серверов и центров обработки данных. Cloudflare способна отслеживать различные киберугрозы и аномальную активность в Сети.

За шесть раундов венчурного финансирования компания привлекла более $330 млн. В прошлом году говорили о ее возможном IPO в первой половине 2019 года, но размещение перенеслось на осень. Последний инвестраунд в марте принес Cloudflare $150 млн.

Netskope

Фирма предлагает другим предприятиям услуги безопасного доступа в облако (CASB). Netskope Security Cloud защищает любые типы облачных сервисов, конфиденциальные данные в Сети и предотвращает киберугрозы. На облако Netskope перешли уже 25% компаний из списка Fortune 100.

Сейчас оценка стартапа превысила $1 млрд. Генеральный директор Netskope Санжай Бери уже заявил о том, что IPO стоит в планах компании, но не уточнил сроки. Мы ожидаем его ближе к концу 2020 года.

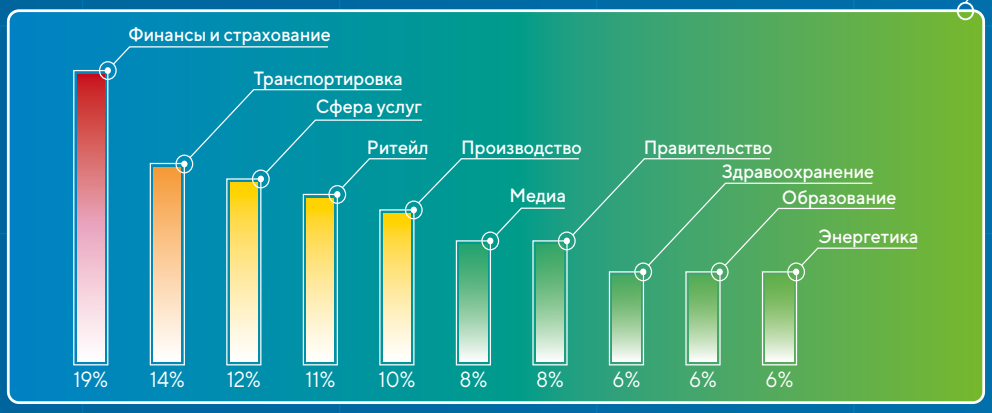
SentinelOne

Платформа использует искусственный интеллект для обнаружения и блокировки новых видов вредоносных программ и хакерских атак. За шесть раундов венчурного финансирования SentinelOne привлекла $229,5 млн. Основной конкурент SentinelOne компания CrowdStrike уже разместилась на бирже NASDAQ в мае этого года. Генеральный директор SentinelOne Николас Уорнер заявил, что IPO возможно в ближайшие несколько лет, но сейчас главная цель — достичь положительного денежного потока.

ExaBeam

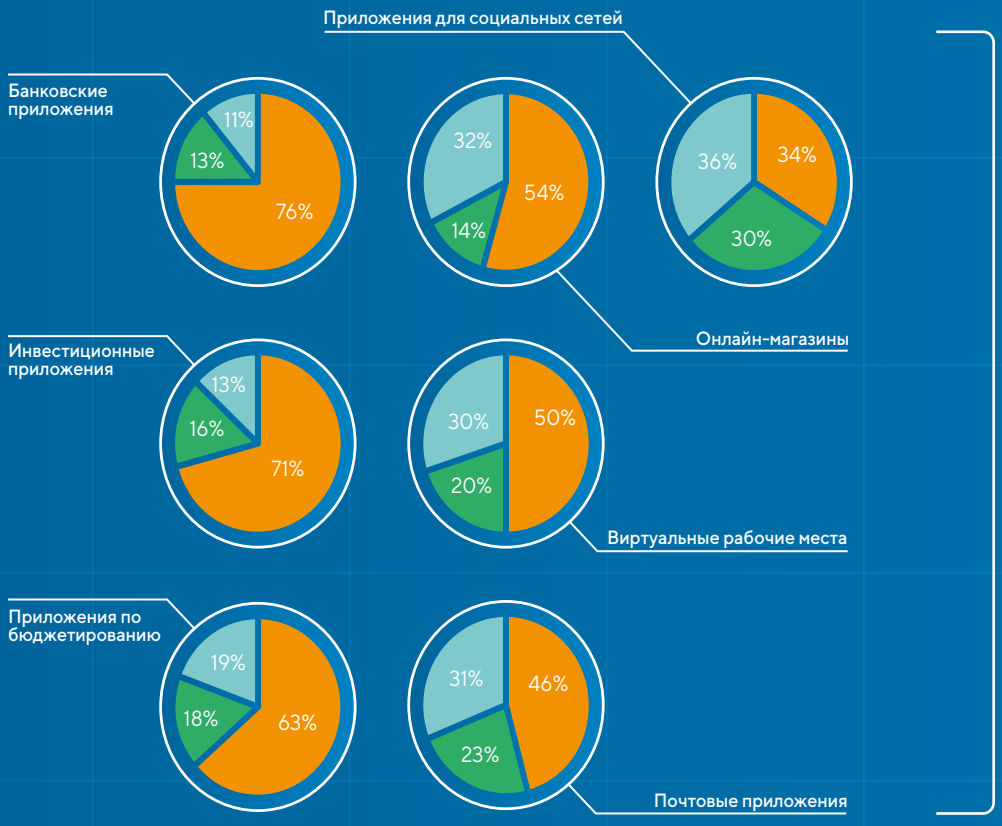
Компания из калифорнийского города Сан-Матео. Ее основной продукт — платформа по управлению безопасностью со встроенной системой реагирования на кибератаки, которая централизует информацию и позволяет обнаружить аномальную активность, идущую как с устройств работников компании, так и извне.

ExaBeam находится на поздней стадии венчурного финансирования, а всего с 2013 года в нее было вложено $190 млн. Генеральный директор Exabeam Нир Полак заявил о росте бизнеса на 300% в 2016 году, на 250% — в 2017-м и более чем на 200% — в 2018-м. В этом году он прогнозирует $100 млн дохода. По данным Pitchbook, предварительная оценка компании составляет $820 млн. Аналитики ожидают IPO платформы ExaBeam уже в следующем году.



Доля компьютерных атак, приходящихся на ту или иную отрасль экономики по итогам 2018 г.

Источник: отчет IBM 2019

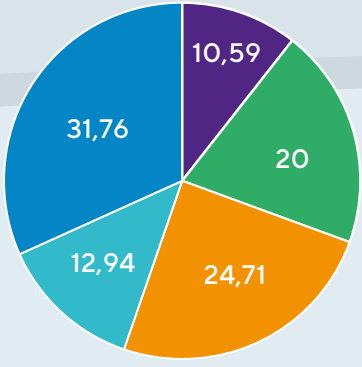


Приложения или аккаунты, вызывающие у респондентов обеспокоенность в отношении:

- Безопасности в целом
- Приватности
- Уязвимостей, связанных с упрощенным использованием

Источник: отчет IBM 2019

Изменение бюджета российских банков на информационную безопасность*



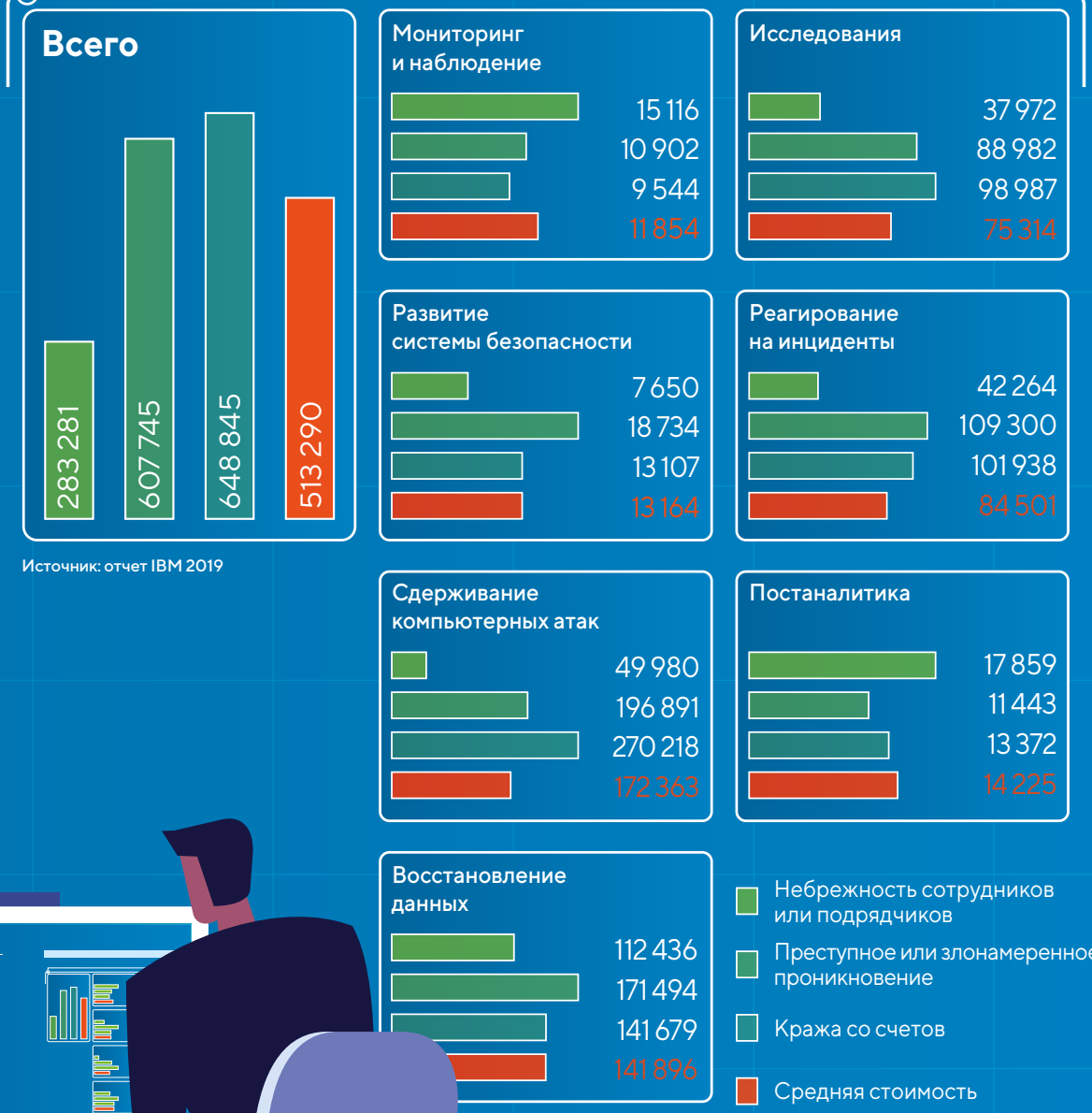
- Рос 2 года подряд
- Вырос в 2017 г., но не рос в 2018 г.
- Вырос в 2018 г., но не рос в 2017 г.
- Не изменился с 2016 г.
- Нет данных

* от общего количества банков

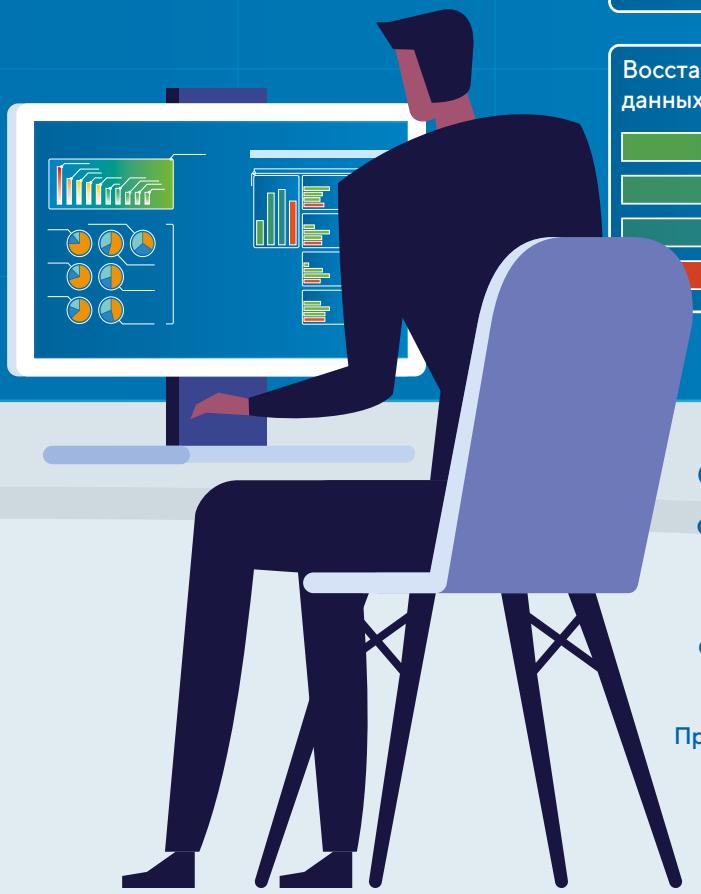
Источник: Qrator Labs

Расходы крупных компаний на кибербезопасность

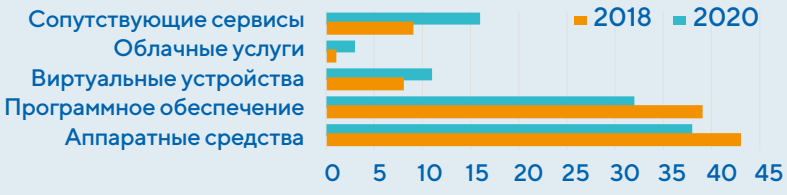
Средние расходы на защиту от киберпреступлений (на 1 инцидент), $



Источник: отчет IBM 2019



Оценка секторов мирового рынка средств обеспечения информационной безопасности, %



Источник: Canalys Estimates, Cybersecurity Analysis, 2018

Облако под защитой

Почему инвесторы полюбили акции компании Zscaler

Никита Гришунин,
старший персональный менеджер
ИК «Фридом Финанс»

В современном мире, где число подключенных к интернету устройств превышает население Земли, сложно гарантировать конфиденциальность любой информации, будь то паспортные данные частного лица или запатентованная технология по производству новейших лекарств.

Именно поэтому с каждым годом растет количество частных лиц и бизнесов, нуждающихся в обеспечении безопасности своих данных. Помочь им с этой проблемой могут облачные решения. Сейчас на них приходится 17,6% от общей стоимости рынка кибербезопасности, хотя годом ранее они составляли лишь 13,8%. По оценкам исследовательской компании Grand View Research, сегмент облачных решений при среднегодовом темпе роста в 13,9% достигнет объема в $8,9 млрд к 2020 году, а к 2024 году будет составлять уже $12,64 млрд.

Мал, да удал

Основным новатором и лидером в этой сфере стала компания Zscaler, вышедшая на IPO весной 2018 года. Она разместилась на бирже NASDAQ под тикером ZS в марте, и за полтора года ее акции подорожали более чем в два раза, а капитализация приблизилась к $10 млрд.

Успех кроется в уникальной продукции. Компания предлагает два основных решения: Zscaler Internet Access (ZIA) и Zscaler Private Access (ZPA). ZIA надежно соединяет пользователей с приложениями, управляемыми извне. ZPA предлагает авторизованным пользователям безопасный и быстрый доступ к приложениям с внутренним управлением, размещенным в центрах обработки данных предприятия или в общедоступном облаке.

Клиенты Zscaler могут защитить своих пользователей путем маршрутизации интернет-трафика через Zscaler Security Cloud, который распределен по 100 центрам обработки данных по всему миру. Прямая облачная архитектура компании связывает пользователей с ближайшим центром обработки данных Zscaler, что ускоряет общее взаимодействие. Этот метод также снижает затраты для клиентов, поскольку им не нужно приобретать собственный набор устройств сетевой безопасности и управлять им.

В рейтинге Gartner комания становится лидером среди облачных служб безопасности веб-шлюзов восьмой раз подряд. Исследователи отдавали Zscaler 55% рынка по состоянию на 2017 год. Среди конкурентов Zscaler можно выделить такие компании, как McAfee, Symantec и Cisco. Они успешно работают в индустрии кибербезопасности, но не все предоставляют услуги облачной безопасности в схожем формате с Zscaler.

Лидерство в своей сфере позволяет на фоне растущего рынка показывать впечатляющие результаты. В III фискальном квартале 2019 года выручка компании выросла на 55% в годовом исчислении, до $84,7 млн, а прогноз на весь год предполагает рост бизнеса на 57%, до $300 млн.

Продукт Zscaler, несмотря на разработки конкурентов, все еще остается уникальным, поэтому фирма оправдывает выбор своих инвесторов, продолжая их радовать как своими операционными, так и финансовыми показателями.

Zscaler. Штаб в Кремниевой долине. Источник: shutterstock.com

АВТОСТРАХОВАНИЕ ЗА 5 МИНУТ ONLINE

ПОЛНАЯ ЗАЩИТА АВТОМОБИЛЯ
ОТ МЕЛКИХ ЦАРАПИН ДО УГОНА

FREEDOM finance | Insurance

5777 www.ffins.kz

Информационная безопасность — приоритет ФФИН Банка

Заместитель Председателя Правления ФФИН Банка Владимир Почекуев — о том, почему клиенты банка могут быть спокойны за свои деньги и личные данные

Владимир Почекуев, заместитель Председателя Правления ФФИН Банка

Владимир, какие направления в области защиты данных клиентов сейчас наиболее актуальны для российской банковской сферы?

Банк России существенно повысил внимание к мерам защиты персональных данных и безопасности банковских транзакций. Так, регулятор предписал банкам быть готовыми к внедрению технологий биометрической идентификации, и мы, безусловно, к этому готовимся — уже провели переговоры с несколькими вендорами. Планируем внедрить такую возможность в нашем флагманском отделении, которое скоро откроется на первом этаже башни «Меркурий» в «Москва-Сити». Сейчас идет настройка программного обеспечения.

Конечно, технология достаточно сложная, и ее внедрение займет куда больше времени, чем предполагал ЦБ. Но она может позволить сделать многое, и сейчас мы думаем о том, как можно было бы ее применить на практике.

Фактически мы говорим об удаленной идентификации клиента вроде технологии Face ID. Записав лицо и голос клиента в специальную базу, мы легко сможем его верифицировать.

Правда, возникает вопрос, насколько эта технология будет удобна клиентам и применима на практике. Дело в том, что банки придумывают все новые технологии защиты, а мошенники находят все новые способы обойти это — и так по спирали. Важно оценить эффективность данной технологии по отношению к размеру затрат и решаемым задачам. Мы коммерческая организация и действуем в первую очередь в интересах наших бенефициаров.

Периодически в СМИ проходит информация о взломе банковских систем и краже информации о клиентах. Стоит ли это воспринимать как трагедию?

Для банков это, конечно, трагедия. Ведь банк — организация, которой доверяют определенную ценность: деньги и информацию. Если банк не смог эту ценность защитить, то доверие теряется не только к банку, но в целом к банковской системе, потому что клиент зачастую смотрит на нее как на нечто целостное. И бьет это по репутации всех игроков рынка, хотя они используют разные технологии.

Как вы оцениваете степень «сетевой обороны» банка?

Оцениваю как крайне высокую. Наши клиенты могут быть спокойны. Информационная безопасность в целом и сетевая защита в частности — один из приоритетов всей группы «Фридом Финанс».

Мы инвестируем значительные средства в развитие и совершенствование мер информационной безопасности: закупаем дорогостоящее шифрующее оборудование и специальное программное обеспечение, получаем специальные лицензии, приглашаем специалистов из компаний-поставщиков (Cisco), получаем консультации от экс-сотрудников госбезопасности.

Регулятор в последние несколько лет выпустил много нормативных документов и во время своих проверок банков уделяет значительное внимание как существующим, так и планируемым мерам. Да, это повышает регуляторную нагрузку, но абсолютно правильно. Сохранность информации — фундаментальная составляющая любого банка.

Более того, регулятор стал более активно подталкивать банки к улучшению их системы защиты данных. Мы разделяем этот подход, хотя приходится соответствовать постоянно растущим стандартам.

Я приведу простой пример: у банка есть сертификат PCI DSS Level 1, который дает нам право хранить данные карты для обработки транзакций без повторного введения информации по карте. Для получения сертификата необходимо пройти аудит на соответствие формальным требованиям со стороны платежных систем — как нормативного (например, регламентация доступа к тем или иным системам), так и технического характера (внедрение определенного оборудования, программного обеспечения, прохождения специальных тестов).

Это формальные и минимально необходимые требования, и мы их выполняем. Но помимо этого мы внедряем дополнительные меры безопасности, которые от нас никто не требует. Это могут быть как собственные разработки, так и решения с рынка. По ряду направлений у нас есть значительная экспертиза, отличная команда с уникальным опытом.

О хакерах и атаках мы знаем не понаслышке: нас пытались взламывать, и не раз. И нам всегда удавалось успешно отбиваться и обеспечивать должную защиту. Наши клиенты об этом даже не знали: работа сервисов практически не останавливалась. Это очень ценно.

Как будет развиваться продуктовая линейка с учетом все более высоких требований к обеспечению безопасности данных?

Я полагаю, что сбор биометрии, данных о поведении клиента, информация о его предпочтениях и так далее задают два потенциальных вектора развития продуктов.

Первый вектор — это характеристика продукта, например его стоимость для клиента. Это уже работает: страховые компании делают клиенту скидку на КАСКО, если у него не было аварий или если он предоставил доступ к данным о своем перемещении через мобильное приложение.

Банки также начинают использовать эти данные в анализе клиентов — в частности, чтобы принять решение о выдаче кредита. Мы как инвестиционный банк больше сфокусированы на оказании расчетных услуг, поэтому данный вектор для нас не в приоритете.

Второе направление развития продуктов — доступность и уровень сервиса. Например, благодаря биометрии мы сможем открывать счета дистанционно, дополнительно верифицировать клиента при контакте с ним через отделение, приложение или банкомат. По данному направлению мы уже внедрили или собираемся внедрять некоторые изменения. Например, система «свой — чужой» позволяет не пустить в мобильный банк обращение, если оно сделано не с доверенного устройства. Также мы внедряем систему для звонков через приложение банка по защищенному соединению. Как мы знаем, при обычном звонке через оператора передаваемые конфиденциальные данные не защищены. Это и многое другое позволит сделать банковские продукты доступнее и сможет повысить качество сервиса.

Однако для меня самым важным критерием является практическая применимость, удобство — то, насколько инновация поможет клиенту, какую его проблему решит, не создаст ли дополнительных сложностей в обслуживании. Не все инновации приживаются, а иногда приживаются те, которые казались неудобными. Здесь очень узкий зазор между защитой информации, дополнительной гарантией безопасности и простотой, свободой личности, ее правами. И важно найти баланс.

Какие простые правила надо знать любому владельцу пластиковой карты, чтобы себя обезопасить?

Надо понимать, что оплата картой при соблюдении простых правил всегда более безопасна, чем оплата наличными. Владелец карты всегда может обратиться в банк, выпустивший карту, и опротестовать списание суммы, если у него есть на то основания. В случае оплаты наличными вернуть средства далеко не всегда возможно.

Основные правила пользования картой:

- Не фотографируйте, не отправляйте данные карты кому-либо, не сообщайте информацию, выбитую на карте, кому-либо — даже сотрудникам банка.
- При оплате в магазинах, ресторанах, кафе, отелях не выпускайте карту из виду, а при оплате самостоятельно вставляйте карту в терминал и не позволяйте ее уносить. Если терминал не переносной — проследуйте до кассы.
- Около банкомата проверьте, нет ли «ридера» (насадки) на диспенсере карты. Если обнаружили — не вставляйте карту, а сообщите в банк, который владеет банкоматом.
- В интернете совершайте оплату только в проверенных магазинах, которые дорожат репутацией. Хороший совет — завести дополнительную карту для оплаты покупок в интернете. К слову, мы позволяем выставить лимиты по карте (на операцию, на день, на месяц и т. д.), чтобы минимизировать риски.
- И последнее: не храните все деньги на одной карте. Откройте расчетный счет и переведите значительные суммы на него. При необходимости переводите деньги на карту. ФФИН Банк открывает каждому клиенту 3 счета в 3 валютах и 3 обычных расчетных счета — в том числе по этой причине.

«Идеальных антивирусов не существует, но и замены им нет»

Ведущий аналитик отдела развития компании «Доктор Веб» Вячеслав Медведев — о безопасности в Сети и сетевой гигиене

Вячеслав Медведев, ведущий аналитик отдела развития компании «Доктор Веб»

Вячеслав, оцените важность сетевой безопасности сегодня?

В условиях, когда в сети Интернет простейшим запросом в поисковике можно найти все необходимое для атаки на компанию, важность защиты сложно переоценить.

Методы атак давно отработаны и подробно описаны. Вредоносные программы разрабатываются и тестируются под заказ, сервисы для вывода награбленного, в том числе найм «мулов» для вывода денег, работают как часы — и никто не предпринимает мер по закрытию этих ресурсов в русскоязычной части Сети (в англоязычном сегменте подобные сайты практически отсутствуют).

Сформулируйте наилучший, на ваш взгляд, подход к обеспечению корпоративной безопасности?

Если бы кто-то придумал рецепт от всех болезней, то давно бы наступило всеобщее счастье. В подавляющем количестве компаний для защиты используется один антивирус, а средства резервного копирования применяет только каждая десятая компания. И при этом практически все уверены в том, что существует где-то идеальный антивирус, который ловит на 100% все вредоносные программы в момент попытки их проникновения, даже не запуска. Что недостижимо даже теоретически.

Если вы думаете, что хакеры — это передовой отряд исследователей, то вы не правы. По данным МВД РФ, настоящих хакеров-исследователей, пишущих новейшие вредоносные программы, порядка 10 человек на всю страну. Все остальные — это в своей массе непрофессионалы, желающие заработать.

Да, продвинутые группировки существуют, но правят бал крайне примитивные атаки типа рассылок вредоносных программ с помощью спама или заражения сайтов.

Вы работаете не только в России. Чем отличается индустрия безопасности здесь по сравнению с другими государствами?

Люди везде остаются людьми, социальная инженерия работает везде одинаково. Разница в активности самого общества. За рубежом инициаторами многих мер являются самые разные группы — от групп родителей до профессиональных объединений. У нас же меры защиты спускаются сверху и с ходу отвергаются обществом — вне зависимости от того, реально нужны они или нет.

В результате, как уже мы писали, за рубежом хакерских сайтов практически нет, а на русском языке их огромное количество. На Западе хакеры садятся на серьезные сроки, у нас отделываются условными.

Если говорить об обычных пользователях, какие правила надо знать для снижения рисков работы в Сети?

Необходимо устанавливать обновления, чтобы закрыть уязвимости. Наша статистика показывает удивительный факт: вторая по популярности уязвимость, используемая злоумышленниками, известна уже семь лет! Но обновления для нее так и не установлены у большинства пользователей.

Не используйте в работе права администратора — в таком случае большинство методов атак окажется неактуальным.

Не запускайте программы из писем.

В браузерах и офисном ПО отключите по возможности использование скриптов — программ, расширяющих функционал документов или сайтов, организующих их поведение.

Делайте резервные копии важных данных.

И, естественно, используйте антивирус — универсальную защиту, замены которой в настоящее время нет.

«Выживут не все»

Почему технологии должны помогать в охоте за киберпреступностью, а не в пассивной защите от нее, объясняет Антон Фишман, руководитель департамента системных решений компании Group-IB, специализирующейся на предотвращении и расследовании кибератак

За последние 10–15 лет рынок кибербезопасности изменился кардинально. Это связано с постоянной «гонкой вооружений». Киберпреступность образца начала 2000-х — это 1-2 энтузиаста, которые самостоятельно разрабатывали необходимые модули и были ограничены в информации, технологиях и средствах. Поэтому для защиты от атак хватало антивирусов, систем обнаружения вторжений и межсетевых экранов.

Сейчас киберпреступность — международный супермаркет с огромным количеством участников со всего мира, которые объединяются в устойчивые киберкриминальные группировки, нанимают персонал, арендуют и покупают сложное вредоносное ПО, состоящее из различных модулей и компонентов.

Только одну такую вредоносную программу могут разрабатывать десятки людей, и для ее «кастомизации» уже не требуется замены бóльшей части кода. Теперь способность обходить защиту — такое же неотъемлемое требование к софту, как, например, качество картинки — к телевизору.

Поэтому подходы к сетевой безопасности тоже меняются. Программы давно работают не только «сигнатурно», то есть определяют вирусы по характерным признакам, но и анализируют аномалии в трафике, поведение объектов, учитывают, что вредоносный трафик способен скрываться в виде других популярных и разрешенных протоколов и программ. Кроме того, злоумышленники не брезгуют и легальным софтом — например, для системных администраторов. Человеческий фактор также часто работает в пользу злоумышленников.

Уязвимости и угрозы «нулевого дня» (например, вирусы-шифровальщики или целевые атаки) — такой же товар на черном рынке, как наркотики и оружие. Современные средства предотвращения кибератак обязаны учитывать все это, своевременно обнаруживать потенциальные проблемы и бороться с ними.

В будущем гонка кибервооружений обострится. Выживут те компании, которые построят единую экосистему кибербезопасности, закроют не точечные, а все доступные каналы, учтут широкий спектр направлений атак,

Антон Фишман, руководитель направления системных решений компании Group-IB

внедрят алгоритмы машинного обучения и будут выявлять инциденты даже в условиях неполных данных.

Будущее — за интеллектуальными сервисами, которые способны принимать решения без участия людей. Новая парадигма работы систем защиты заключается не в том, чтобы помочь клиенту пережить атаку с наименьшими потерями, а в том, чтобы предотвратить киберпреступление вообще.

Поэтому наиболее прогрессивные представители индустрии используют технологию ThreatHunting, занимая проактивную позицию, то есть охотятся за хакерами, следят за их инфраструктурой, активностью, чтобы предугадать и спрогнозировать готовящуюся атаку.

Ну и, наконец, сами люди должны вести себя более ответственно, когда речь идет о безопасности их личных данных.

Банки: скрытая угроза

С какими киберугрозами чаще всего сталкиваются банки и как они научились на них... зарабатывать

Вячеслав Степанов,
заместитель директора
департамента по работе с клиентами
ИК «Фридом Финанс»

Совокупный ущерб от киберпреступлений в мире оценивается в $2,5 трлн, то есть 3% мирового ВВП. Основной удар приходится на банки и их клиентов, а также организации, обладающие большим количеством персональных и иных важных данных, в том числе финансовых.

Далеко не все банки могут обеспечить кибербезопасность на высоком уровне. К тому же арсенал хакеров постоянно пополняется: они пользуются «дырами» в оборудовании и программном обеспечении, халатностью персонала или доверчивостью клиентов.

Потерпевшие организации публично не раскрывают потери от киберпреступлений. 80% пострадавших скрывают не только ущерб, но и сам факт успешной атаки. О нем узнают из слухов и прочих неофициальных источников.

Атаки на банки, усилившиеся несколько лет назад, заставили российское государство пересмотреть отношение к интернет-безопасности. В структуре Банка России даже был создан департамент по противодействию киберугрозам. В прошлом году регулятор разработал нормативные указания по оценке рисков информационной безопасности. Предполагается, что с 2020 года риск от киберугроз будет напрямую влиять на капитал банков.

По оценке регулятора, примерно каждая вторая атака нацелена на банк, платежную систему или биржу.

Линии обороны

Основных методов защиты от киберугроз и их последствий сегодня три: самостоятельная защита, внешние подрядчики и просто страхование рисков.

Первый контур защиты — это отдел собственной информационной безопасности. На его плечи возлагается работа по защите данных от несанкционированного доступа извне и изнутри. Штат отдела может быть довольно внушительным. Например, в службе информационной безопасности Сбербанка сегодня трудятся 1100 человек, или 0,3% от общей численности персонала. На кибербезопасность, по признанию банка, было потрачено 1,5 млрд рублей, что превышает 0,1% всех операционных расходов.

Второй периметр информационной безопасности выстраивается силами внешних партнеров. Банкам в любом случае требуется защита от DDoS-атак, спама и прочих угроз. На этом этапе незаменимы услуги операторов связи, облачных провайдеров. Кроме того, существуют и специфические услуги, например такие, как поиск по Даркнету важной информации, которая позволяет предотвратить или минимизировать ущерб. Например — о появлении в продаже на черном рынке базы данных клиентов банка, их учетных данных, номеров карт.

При этом, по данным Group-IB, почти три четверти банков в России не готовы к атакам на свою информационную инфраструктуру. Поэтому последним средством управления рисками киберугроз является их страхование.

Потребителями этой услуги могут быть не только крупные корпоративные заказчики, но и частные лица. Полисом киберстрахования покрываются риски, которые банк по договору с клиентом не обязан возмещать (например, при краже ПИН-кода).

Два миллиона из более чем 90 млн клиентов самого Сбербанка уже страхуют свои пластиковые карты от мошенничества. Аналогичные продукты есть и у других банков. Полис стоит около 1,5% от страховой суммы в год.

Слабая заинтересованность населения в этой услуге пока связана с непониманием угроз кибербезопасности и их недооценкой. Кроме того, банки пока что не в состоянии полностью переложить все риски хищения средств на самих клиентов. Но в будущем киберстрахование вполне может стать такой же стандартной услугой, как ОСАГО.

А банки, в свою очередь, будут на этом хорошо зарабатывать.

Источник: shutterstock.com

FREEDOM finance

Лицензия на осуществление деятельности на рынке ценных бумаг 3.2.238/15 от 02 октября 2018 года. www.almaty-ffin.kz. Реклама.

ffin.kz

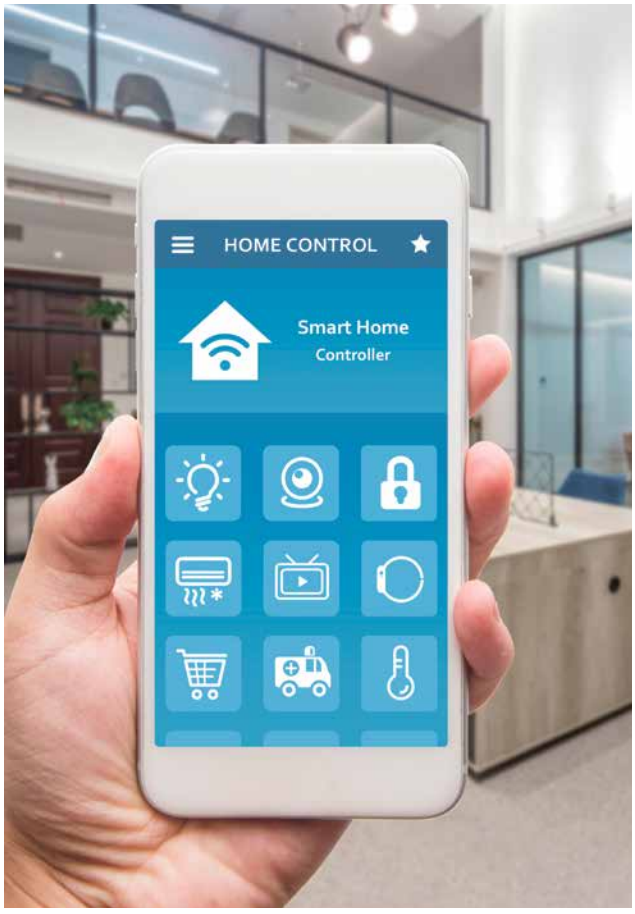
7555

Кто в доме за хозяев

Новые технологии делают семейный быт не только умнее, но и безопаснее. Станут ли они для международных IT-гигантов новой золотоносной жилой или источником головной боли?

Георгий Волосников,
директор департамента по работе с клиентами ИК «Фридом Финанс»

Развитие технологий «умного дома» уже меняет наши представления о способах обеспечения безопасности жилья. Решения становятся проще благодаря всеобщей информатизации и открывают дорогу для роста бизнеса технологических гигантов на этом поле.
Однако у этого процесса есть обратная сторона — всевозможные риски, главным из которых является утечка личных данных.



Источник: shutterstock.com

Тук-тук

«Умным домом» сейчас вряд ли кого-то можно удивить. Развитие рынка интернета вещей и распространение смартфонов породило массу интересных решений по контролю за личной собственностью. «Умные» датчики, сенсоры, двери, замки, камеры видеонаблюдения позволяют пользователям знать о состоянии дел дома 24 часа в сутки в любой точке мира. Технологический прогресс сделал эти решения доступными многим как по цене, так и по сложности функционала.
Большинство технологических гигантов вроде Amazon, Google, Apple, Samsung или Xiaomi предлагают пользователям собственные системы «умных домов», которые призваны увеличить безопасность жилья. В центре подобных экосистем для дома зачастую оказываются голосовые помощники, так что не за горами время, когда на смену консьержам придут Алисы, Сири и Алексы.
Одним из лидеров индустрии является онлайн-ритейлер Amazon. Безопасный дом может улучшить и безопасность доставки товара, что положительно скажется на выручке. К тому же голосовой помощник Алекса способен замкнуть пользователя в экосистеме компании, что означает потенциальный рост рекламных доходов и возможность анализировать данные пользователей.
Представьте, что купленные в онлайн-магазине продукты сразу отправляются в холодильник и клиенту не приходится ждать курьера. Пока развитию сервиса до такого уровня не хватает безопасности. Люди закрывают дом при уходе и не могут открыть дверь курьеру. А что, если делать это дистанционно?
Для реализации подобного сервиса Amazon приобрел две крупные компании. В 2017 году за $13,5 млрд к нему присоединилась сеть супермаркетов органических продуктов Whole Foods, в феврале 2018-го — стартап Ring, купленный за $1-1,8 млрд.
Ring производит «умные» дверные замки с видеокамерой, которые можно установить самостоятельно. Стартовый пакет от Ring для защиты дома стоит в США $200.

Сервис по дистанционному управлению дверьми и видеонаблюдением Amazon уже реализует в проекте Amazon Key, так как с развитием покупок онлайн участились случаи пропажи доставленных товаров. Однако для скоропортящихся продуктов компании не хватало компонента в ее системе, и, возможно, стартап Ring с инвесторами из России и украинскими разработчиками станет тем самым компонентом.

Главным конкурентом системам Ring от Amazon в США считается Nest Secure от Alphabet. В 2014 году Google приобрела Nest за $3,4 млрд, поскольку тоже видит большой потенциал в сфере безопасности «умных домов». И это неудивительно, ведь, по прогнозам аналитиков Market Research Future, мировой рынок систем домашней безопасности будет расти со средним темпом 9% в год и к 2023 году составит $55 млрд.

Похожие решения есть и у Apple с «умной» камерой. Samsung делает продукт SmartThings и работает в партнерстве с компанией ADT, которая занимается обеспечением безопасности домов. Скоро свое решение представит и российский «Яндекс».

Незваные гости

Однако технологический прогресс несет в себе и риски. Наиболее очевидные из них — хакерские атаки и потеря личных данных.

В начале 2019 года разгорелся скандал вокруг видеозаписей с устройств Ring. Оказалось, что украинские разработчики компании имели возможность просматривать видео с любого установленного устройства в любой точке мира. Хотя это было сделано для исправления ошибок сверхчувствительности датчиков, случалось, что инженеры делились рассказами о том, кто из клиентов и с кем пришел домой после вечеринки.

Компания отрицала наличие проблемы, но сама возможность просмотра другими людьми столь деликатной личной информации поднимает вопрос о безопасности новых систем.

Вопросы приватности становятся все более актуальными, если представить, в какую сторону прогресс может увести технологии видеонаблюдения. Стартап Alarm.com еще в 2017 году предложил дополнить системы «умных домов» дронами. По замыслу разработчиков, в случае срабатывания датчиков безопасности хозяева смогут запустить дрон, чтобы осмотреть дом и участок снаружи. Дело в том, что тревожные сигналы от «умных» сенсоров часто оказываются ложными, поэтому дополнительный технологический элемент в виде проверки дроном сможет повысить эффективность систем.

Всевидящее око

Что не заметит дрон — отследят спутники. Как утверждает издание MIT Techology Review, пока вы читаете эти строки, над нашими головами парит более 2000 аппаратов.Частота запусков увеличится с 365 в 2018-м до 1100 к 2025 году благодаря частным компаниям вроде SpaceX. Космический стартап Илона Маска ставит цель запустить 12 000 спутников к 2027 году.

Удешевление и увеличение их числа, а также развитие линз для телескопов могут сделать видеонаблюдение с неба массово доступным.

Качество картинки из космоса постоянно улучшается, и она уже может использоваться для обеспечения безопасности, пока скорее общественной. Например, в 2013 году полиция в штате Орегон получила сообщение о том, что человек по имени Кертис В. Крофт незаконно выращивает марихуану на своем заднем дворе. Проверить информацию помог сервис Google Earth, затем последовал полицейский рейд.

Технологии в США уже позволяют смотреть на землю с разрешением выше 25 см, более высокая детализация ограничена американским регулятором. Однако конкуренция на глобальном уровне способна это изменить. К примеру, китайские компании уже могут предоставлять изображения с более высоким разрешением.

Пока речь идет только об изображениях, но технологии могут дойти и до видео. Стартап SkyBox, который был куплен Google уже под именем Terra Bella, может снимать HD-клипы из космоса длительностью до 90 секунд. Компания EarthNow, в которую вложился Билл Гейтс, пошла еще дальше и планирует покрыть весь земной шар технологиями видеосъемки в реальном времени.

Более радикальные технологии слежки из космоса предполагают использовать радиолокационные изображения, которые захватываются электромагнитными волнами за пределами видимого спектра. К примеру, облака скрывают Землю, но спутники могут посылать через них специальный сигнал, который отражается от обнаруженного объекта и возвращается на спутник. Система может определить высоту объекта до миллиметра. Ранее подобные технологии были доступны только НАСА и военным, но с прошлого года в США открыли к ним доступ и для коммерческого использования.

С развитием интеллекта домовых систем безопасность данных выйдет на первый план. Подглядывание в дверной глазок их инженерами-производителями однозначно трактуется как нарушение неприкосновенности частной жизни. Но как быть, например, с фотографией спальни, сделанной пролетающим мимо дроном, или со спутниковым снимком автомобиля, въезжающего в гараж?

Ответы на эти вопросы не так очевидны и потребуют новых стандартов по защите частной информации. Иначе мы столкнемся с парадоксальной ситуацией, когда больше безопасности будет означать меньше безопасности. На фоне скандалов с утечкой данных Facebook технологические гиганты Amazon, Apple или Alphabet могут получить от «умных домов» не только миллиардные прибыли, но и острую головную боль, пытаясь защитить частную жизнь своих пользователей.

Будьте в гуще событий с

THE WALL STREET JOURNAL.

подписка по выгодной цене

Подробности на сайте:
wsj.kursiv.kz | wsj@kursiv.kz

Инвестиции: личный опыт

Самостоятельное инвестирование как лучший способ защитить капитал

Игорь Клюшнев,
заместитель генерального директора
ИК «Фридом Финанс»

Парадоксально, но отсутствие инвестиций — это риск. Он связан с тем, что вы недополучаете прибыль, когда на фондовом рынке масса возможностей заработать.

Другой, и не менее важный момент: человек, который не управляет своим брокерским счетом, не получает инвестиционный опыт. Такой опыт может со временем превратиться в мощнейший мультипликатор пассивного дохода. Новичок не заметит перспективную сделку, которую отметит опытный инвестор.

Даже тот, кто в течение трех лет не слишком успешно управлял собственным брокерским счетом, с большей вероятностью научится зарабатывать, чем депозитчик. Негативный опыт поможет избежать ошибок в будущем.

Начало

Открыв счет у брокера и переведя на него деньги, вы сделали важный, но первый шаг. Приготовьтесь к марафону, а не спринту. Успешные инвесторы — это те, кто управляет сбережениями всю жизнь.

Важно, чтобы на брокерском счете были не кредитные деньги и не единственные ваши сбережения.

Для того чтобы разобраться в теме инвестиций, стоит поучиться. Обучающие курсы в брокерских компаниях полезны своей привязкой к практике и разбором рыночных примеров.

Книги также пригодятся. «Разумный инвестор» Бенджамина Грэма, не теряющая актуальности классика, поможет лучше осознать переменчивость рынка и важность системного подхода.

Выбор стратегии

Основной фактор выбора стратегии — возможность регулярно находить время для изучения рынка и совершения сделок.

При отсутствии времени стоит выбрать **пассивное инвестирование.** При таком подходе собирается портфель акций крупных компаний на длительный срок — например, из старейшего американского индекса DJ-30, в который входят 30 компаний. Треть из них была основана еще в XIX веке, а самая маленькая имеет капитализацию $30 млрд.

Есть удобный способ вложиться в акции индекса одной сделкой — купить ETF. Для квалифицированных инвесторов доступен фонд, торгующийся в США, — SPDR Dow Jones Industrial Average ETF. Неквалифицированные инвесторы могут приобрести акции похожего фонда, который торгуется на Московской бирже — это FinEx USA UCITS ETF.

Стратегия при пассивном инвестировании соответствует принципу «купил и держи» (Buy and Hold). То есть инвестор периодически докупает ценные бумаги, рассчитывая на их долгосрочный рост.

Среднегодовая доходность индекса DJ-30 с 1896 года составляет порядка 9% в долларах.

Активное инвестирование

Этот подход предполагает разделение портфеля: 70-80% денег идет на покупку ETF на индекс DJ-30, а на оставшиеся 20-30% формируется портфель из компаний средней и малой капитализации. Это позволяет повысить среднюю доходность портфеля, так как небольшие компании меняются в цене гораздо сильнее крупных, уже устоявшихся бизнесов. Помочь с выбором перспективных бумаг может инвестиционный консультант «Фридом Финанс».

Ожидаемая доходность от активного инвестирования составляет 12-15% годовых. Также стоит понимать, что растет риск просадки портфеля ниже среднерыночного значения.

Трейдинг

Потребует ежедневного мониторинга новостного фона. Трейдер покупает акции на периоды от нескольких минут до нескольких недель. Выбор бумаг широк — не меньше 2000 ликвидных акций, если речь идет об американском рынке. К слову, почти все они доступны для неквалифицированных инвесторов на Санкт-Петербургской бирже.

Выбор моментов для совершения сделок в трейдинге нередко связан с проведением технического и новостного анализа. Ориентир по доходности — 20% годовых.

Все три подхода к биржевому делу помогут накопить полезный инвестиционный опыт, который научит находить интересные инвестиционные идеи и зарабатывать на них, защищая капитал от инфляции и других рисков.

«Чтобы подобрать восьмизначный код к счету в TraderNet, потребуется 20 тысяч лет»

Основатель сервиса Денис Матафонов рассказывает о системе защиты биржевой платформы и объясняет суть ее работы

Денис, в чем заключается уникальность платформы TraderNet?
TraderNet — это биржевой агрегатор, который может подключаться сразу к нескольким торговым площадкам России, СНГ, всей Европы, Америки. Внутри платформы работают сервисы по учету остатков в нужных валютах, обсчитываются денежные лимиты, ведется CRM-учет.
Плюс ко всему платформа поддерживает 5 дополнительных языков: английский, немецкий, польский, болгарский, турецкий. Конечно, существуют решения, которые позволяют подключаться к каждому рынку отдельно, однако такой широкий функционал и мультидоступ предоставляет только TraderNet.

Насколько безопасно пользоваться TraderNet? Какие технологии безопасности используются внутри платформы?
TraderNet поддерживает четыре разных варианта защиты: это смс-пароль, виртуальный и физические криптоключи, разработанные нашими программистами специально для пользователей, плюс электронно-цифровая подпись. Также мы используем общие параметры безопасности: логин, пароль, динамическое подтверждение операций — отправка смс.
Несмотря на то, что последний способ наиболее известен, проблемы, связанные с ним, распространены не менее широко. В случае обрыва связи этот сервис становится неактивным, что, в свою очередь, приводит к сбоям в отправке-получении смс-уведомлений. Более того, эта услуга платная и для клиента, и для банка.
Также стоит отметить, что каждое подтверждение пароля на уровне верификации замедлено. Когда вы загружаете TraderNet, сам по себе вход в платформу занимает время. И это сделано специально для того, чтобы нельзя было быстро подобрать пароль.

Денис Матафонов, основатель сервиса TraderNet

Чтобы подобрать восьмизначный шифр, потребуется 20 тысяч лет. Поэтому мы стараемся не мучить клиентов и использовать устойчивые простые решения. Наличие современной двухфакторной аутентификации, также используемой нами, не позволит злоумышленнику нанести ущерб.

По требованиям американских аудиторов мы обязаны соблюдать самые высокие рекомендации по безопасности. Созданное нами криптографическое хранение ключей (токены) на клиентских устройствах обеспечивает максимальную защиту данных.
В то же время мы выдерживаем баланс между безопасностью и удобством в использовании.

FREEDOM finance

Лицензия на осуществление деятельности на рынке ценных бумаг 3.2.238/15 от 02 октября 2018 года. www.almaty-ffin.kz. Реклама.

ffin.kz

7555

Виртуальная оборона

Насколько опасна мировая киберпреступность и сколько тратят корпорации на борьбу с ней

Владимир Козлов,
директор департамента продаж
инвестиционных продуктов
ИК «Фридом Финанс»

Цифровизация — один из главных трендов нашей жизни, в которой остается все меньше частного пространства. Денежные переводы, обмен фото, видео, личная переписка, конфиденциальные данные — вся эта информация теперь находится в зоне риска, так как способна в любой момент стать добычей киберпреступников. Причем источником утечки может стать как домашний компьютер, так и серверы различных компаний — банков, страховых, просто работодателей и т. д., — которые по долгу службы собирают и хранят огромные массивы личной информации клиентов. Такое хранение требует серьезных затрат на безопасность. Давайте разберемся, насколько они велики и хватает ли этих денег для поддержания кибероборонды.

Цена вопроса

Сначала отделим вынужденные издержки компаний на кибербезопасность — персонал, оборудование, ПО — от размера ущерба, который получит бизнес в случае успешной атаки.

В 2017 году средний размер урона, который наносила вредоносная программа, сумевшая проникнуть во внутренние сети, составил $2,4 млн. При этом на устранение последствий проникновения у компании обычно уходило порядка 50 дней. Почти половина ущерба — это потеря данных. Суммарный же мировой ущерб от действий кибервымогателей превысил $5 млрд, то есть стал в 15 раз выше показателя за 2015 год. Средний ущерб на одного пользователя составлял около $141.

Наиболее крупное киберпреступление произошло с мая по июнь 2017 года в отношении компании Equifax, которая занимается аналитикой данных по кредитным историям. В ходе успешной кибератаки компания не смогла защитить данные 143 млн пользователей в США и 400 тысяч пользователей в Англии. Потери бизнеса составили $4 млрд.

Ожидается, что ущерб от киберпреступлений к 2021 году вырастет до $6 трлн в годовом выражении.

Теперь же перейдем к наиболее актуальному вопросу — что компании делают для предотвращения подобных случаев и сколько это стоит. Средние годовые затраты бизнеса по всему миру на кибербезопасность оцениваются на уровне $10-11,7 млн на компанию. Вступление в силу Общего регламента по защите данных в ЕС вынудило работающие в Европе фирмы затратить порядка $1 млн каждую на подготовку его внедрения.

В структуре базовых расходов фаерволы и сенсорные системы по отслеживанию атак стоят порядка €100 тысяч в год. Еще около €1 млн придется потратить на оборудование для работы с этими программами. Спрос на специалистов в области кибербезопасности значительно превышает предложение, поэтому расходы на персонал также составят весомую часть сверх названных выше сумм. Согласно исследованию Deloitte, затраты на кибербезопасность компании обычно включают в общий бюджет IT-отдела и в среднем они составляют порядка 12% от него. По данным IDG, порядка 75% компаний имеют объединенные отделы IT- и кибербезопасности и лишь у оставшихся 25% кибербезопасность обособлена в самостоятельную структуру.

Взглянем на вопрос кибербезопасности с точки зрения киберпреступника. В 2008 году Международный институт компьютерных наук, базирующийся в США, провел исследование по спам-аналитике и оценил, что хакеры, управляющие системами спам-рассылок, зарабатывают на них порядка $3 млн в год.

Помимо писем «ключом к замку» для хакеров стала инициатива многих компаний по допуску мобильных устройств сотрудников во внутренние системы (Bring Your Own Device, или BYOD Model). К страху многих «безопасников», она буквально уничтожает любой выстроенный периметр киберзащиты и провоцирует одновременное появление множества уязвимостей в системе, когда вирусы через инициированный телефон способны свободно попадать в корпоративную сеть.

Также на стороне хакера играет тот факт, что никто не собирает аналитику по неудавшимся кибератакам, поэтому он может свободно искать брешь в киберзащите фирмы сколь угодно долго — вплоть до побед-

ного конца. Cisco и ряд других организаций, занимающихся кибербезопасностью, отмечают, что порядка 60% вредоносных доменов используется для организации спам-атак на фирмы.

Популярный формат вируса 2000-х годов, известный как троянский конь, составил 53% кибератак на финансовые организации в 2017 году, что подчеркивает уязвимость систем даже к относительно старым разработкам хакеров. Также отмечается, что 92% вирусов до сих пор доставляется по электронной почте, но 77% из них стали «бесфайловыми», то есть для активации вируса нет нужды запускать/открывать какой-либо вложенный файл.

Криптобеда

Взрывной рост индустрии криптовалют открыл перед киберпреступниками новые возможности. Хакерам больше не нужно обходить дорогостоящие системы киберзащиты организаций, выстроенные профессионалами. Зачем это делать, когда можно покопаться на домашнем компьютере жертвы в поисках незащищенного криптокошелька? По данным Global Crypto Press Association, уже к зиме 2017 года хакеры сканировали компьютеры рядовых пользователей, лишенные антивирусов и фаерволов, на наличие в системе файлов под названием Wallet. В случае обнаружения такого файла хакер получал доступ к личному кошельку жертвы, переводил с него деньги на свой кошелек и скрывался. Вернуть утраченное уже было невозможно — в криптофинансовом мире откат транзакции не предусмотрен.

С 2018 года хакерские атаки изменили угол направления. Они перестали красть или вымогать криптовалюту с помощью блокировки функций компьютера. Вместо этого компьютеры начали заражаться вирусами для майнинга электронных денег. То есть после включения компьютера жертва занималась обыденными делами, и в это время его производственные мощности удаленно использовались мошенником для ускорения процедуры создания очередной единицы криптовалюты.

Интересную аналогию привел портал по кибербезопасности The Threat Report. Его автор подметил, что волатильность криптовалюты и ее уязвимость для атак создают для владельца особое видение окружающего мира, полное страха, беспокойства и сомнения. Инвесторы в криптовалюту испытывают ощущения людей, живущих в странах с гиперинфляцией, при ее отсутствии в реальности.

Поэтому все эксперты по кибербезопасности советуют держать кошельки криптовалюты на офлайновых носителях и ноутбуках, отключенных от Сети. Чем дальше от интернета кошелек с криптовалютой, тем крепче сон.

Россия под прицелом

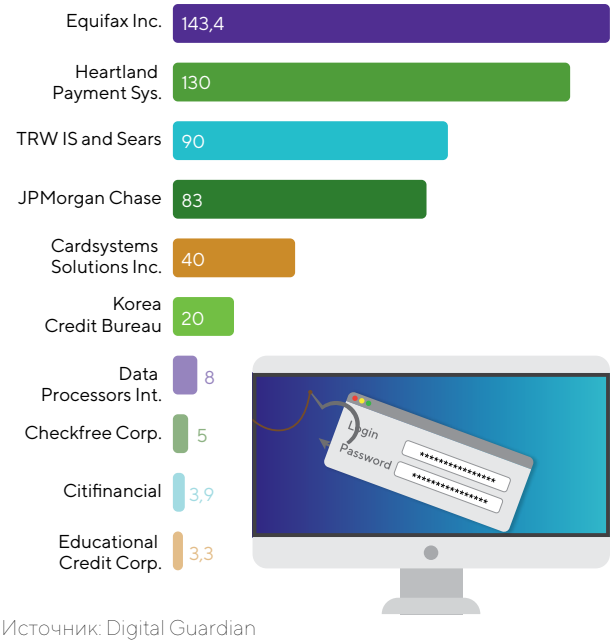
Согласно июньской оценке зампреда правления Сбербанка Станислава Кузнецова, прогнозный объем потерь экономики РФ от кибератак в 2019 году составит примерно 1,6-1,8 трлн рублей. При этом центр киберзащиты банка ежедневно анализирует свыше 6 млрд событий, из них, в том числе с помощью искусственного интеллекта, выделяется примерно 150-200, которые могут представлять угрозу для банка. Учитывая долю Сбербанка в активах банковской системы РФ, в целом по российской банковской системе таких инцидентов происходит приблизительно 450-600 в день, или около 160-220 тысяч в год.

Схожую оценку делает «Ростелеком-Солар». По ее данным, всего за 2018 год в кредитно-финансовых организациях было зафиксировано более 120 тысяч компьютерных атак. Доля критичных инцидентов, то есть способных привести к остановке деятельности или потерям на сумму свыше 1 млн рублей, составила до 19%.

Ежегодные затраты Сбербанка на кибербезопасность, по данным Станислава Кузнецова, составляют до 1,5 млрд рублей. Учитывая рыночную долю ПАО «Сбербанк» на кредитно-финансовом сегменте России, расходы банковского сектора РФ на кибербезопасность можно оценить в 4,5 млрд рублей в год. Не самая крупная сумма, если учесть потенциальный размер потерь.

В целом мировой рынок информационной безопасности будет активно расти в ближайшие годы. С развитием интернета вещей, проекта OneWeb по распространению на земле широкополосного доступа к Паутине и других глобальных инициатив объем информации, которую нужно защищать от киберпреступников, будет постоянно увеличиваться. А это значит, что упомянутые в этом номере «Финансиста» технологические компании имеют все шансы стать фаворитами инвесторов.

Крупнейшие кражи профилей клиентов, млн человек



Источник: Digital Guardian

В зоне доступа

Что делают крупнейшие мировые компании, чтобы личные данные их клиентов оставались надежно защищенными

Антон Мельцов,
директор по развитию
ИК «Фридом Финанс»

«Мистер Цукерберг, не хотели бы вы назвать нам отель, в котором вчера остановились?» — спросил американский сенатор основателя крупнейшей социальной сети Facebook Марка Цукерберга в ходе публичных слушаний в апреле 2018 года. «Эмм… — Самый влиятельный человек в мире по версии журнала Vanity Fair замялся, не зная, что ответить, но потом все-таки четко произнес: — Нет!»

В апреле 2018 года весь мир наблюдал, как глава Facebook, заикаясь и бледнея, отвечал на вопросы представителей верхней палаты Конгресса. Они хотели знать, каким образом личные данные 87 млн пользователей сети оказались без их ведома доступны британской исследовательской компании Cambridge Analytica.

Разразившийся скандал стоил Facebook миллиардов долларов капитализации и штрафов, репутация соцсети была подмочена: оказывается, она не слишком-то серьезно относилась к безопасности личных данных пользователей, несмотря на заверения Цукерберга в обратном.

По результатам 2018 года компания даже решила сменить стратегию развития, переключив тумблер с «максимальной открытости» в положение «закрытость частной жизни». Также компания заявила о предстоящем росте операционных издержек на 50% в 2019 году, так как в рамках новой парадигмы ей необходимо расширить штат и одновременно увеличить затраты на новые дата-центры, которые укрепят передний край обороны сети, защищающий от хакерских атак.

Однако именно «казус Facebook» на сегодняшний день является самым крупным проколом публичной компании, связанным с утечкой данных пользователей.

На самом деле скандал вокруг детища Цукерберга не должен был никого удивить. Опасения сторонников теории заговора уже давно подтвердились: как минимум Соединенные Штаты (да и другие страны) занимаются тотальной слежкой за своими и иностранными гражданами.

Еще в 2013 году работавший на Агентство по национальной безопасности (АНБ) аналитик Эдвард Сноуден раскрыл методы работы американских силовиков с использованием хакеров и вредоносных программ. Причем в скандале были замешаны такие гиганты, как Google, Microsoft, Yahoo и Facebook, которые не мешали АНБ заниматься сбором и обработкой личных данных их клиентов.

Все эти случаи ставят безопасность личной или закрытой корпоративной информации на первое место в эпоху информационного общества. Растет заинтересованность людей и фирм в обеспечении сохранности важных данных. Через 10-20 лет эта услуга будет так же востребована, как сегодня — наличие персонального домашнего компьютера, который в XX веке казался совершенно непригодным для домашнего использования.

Давайте рассмотрим лидеров индустрии безопасности личных данных, которые смогут хорошо заработать на новом тренде.

Cisco Systems (NASDAQ: CSCO)

Публичная компания Cisco является крупнейшим поставщиком услуг сферы кибербезопасности. Ее капитализация составляет порядка $250 млрд и может еще подорожать в будущем вслед за растущим спросом на услуги в сфере кибербезопасности.

По итогам 2018-го выручка компании подросла на 14%, достигнув $49,32 млрд. По оценкам Gartner Group,

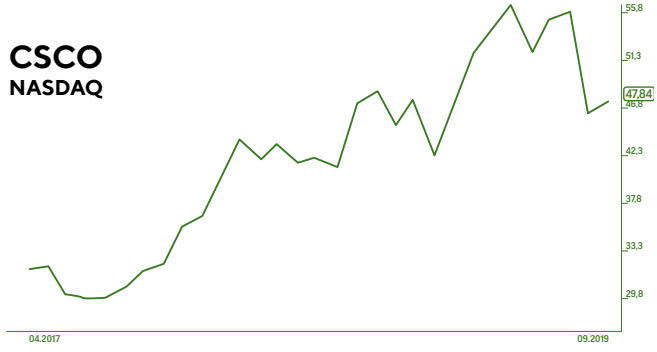


График котировок Cisco Systems

за 2019 год в мире будет потрачено порядка $124 млрд на кибербезопасность, то есть на 8,7% больше, чем годом ранее. Поэтому акции Cisco Systems особо привлекательны, так как компания занимает менее 2% рынка и может значительно вырасти.

IBM (NYSE: IBM)

Компания производит компьютерные мощности и оказывает сопутствующие услуги. У IBM есть разработка в области кибербезопасности под названием QRadar Security Intelligence Platform. Платформа позволяет централизованно управлять сбором информации, обработкой системных журналов, выявлять аномалии, настраивать конфигурации систем и устранять их уязвимости. Сервис активно использует новые методы аналитики и способен применять их на возросших объемах данных. Это помогает выявить инциденты, которые раньше терялись в общем «шуме».

Финансовые показатели компании стабильны. Соотношение чистого долга к прибыли до налогов и процентных отчислений равно 1,86. По ключевому мультипликатору P/E компания торгуется ниже среднерыночных значений — 12,54 против 18,13 в среднем по индексу S&P 500, что может быть обосновано ожидаемым снижением выручки на 3% в текущем году.

Fortinet (NASDAQ: FTNT)

Основанная на заре бума доткомов, компания Fortinet сумела пережить крах интернет-компаний и продолжает развиваться быстрыми темпами. Компания предлагает различные решения в области сетевой безопасности и безопасности облачной инфраструктуры, защиту отдельных точек и т. д.

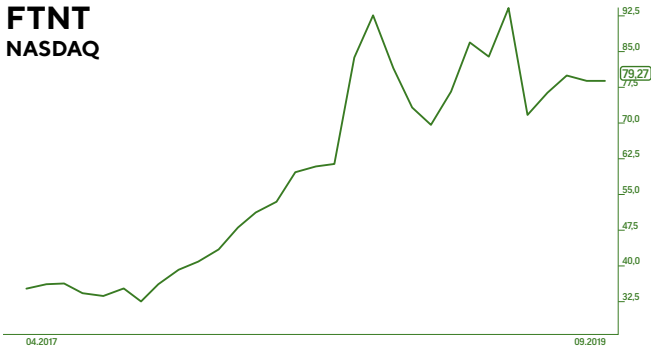


График котировок Fortinet

Благодаря фокусировке бизнеса на конкретном типе услуг выручка компании в текущем году, как ожидается, вырастет на 16%. Как у многих производителей программного обеспечения и сервисов, у Fortinet отсутствует долговая нагрузка. Операционная маржинальность по результатам 2018 года составила 12,83%. Благодаря хорошим финансовым показателям акции компании торгуются на рынке со значительной премией — показатель P/E находится на уровне 39,16.

Accenture (NYSE: ACN)

Формально является консалтинговой компанией, которая предоставляет услуги по организации стратегического планирования, оптимизации и аутсорсинга бизнес-процессов, логистические решения, управление персоналом, а также внедрение IT-технологий. Помимо этого фирма помогает с настройкой управления уже существующей в бизнесе системой безопасности, выявлением киберрисков и обеспечением безопасности приложений и облачных серверов. У Accenture почти нет долгов, а показатель операционной маржинальности стабильно держится на уровне 14%.

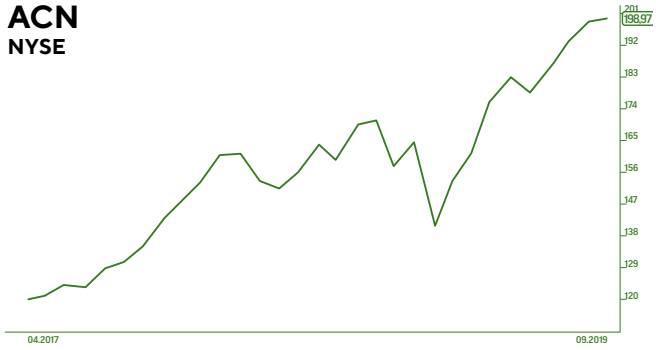


График котировок Accenture

Ожидаемый темп роста выручки в текущем году составляет 3,9%. Так как компания работает в секторе услуг, коэффициент P/E составляет 27,09, что выше среднерыночного значения.

Palo Alto Networks (NYSE: PANW)

Наиболее молодая в нашей выборке компания Palo Alto Networks разрабатывает программы кибербезопасности. Основная продукция — это фаерволы нового поколения, позволяющие детально отслеживать сетевой трафик и предотвращать неизвестные угрозы, а также антивирусные решения для мобильных устройств и компьютеров и сервисы безопасности облачных систем бизнеса.

Одним из самых инновационных продуктов Palo Alto Networks является система Cortex, в которую встроен искусственный интеллект, помогающий адаптироваться под новые угрозы, с которыми сталкивается система. Разработчики также могут создавать собственные приложения на базе системы и анализировать их в Cortex Data Lake.

Ожидается, что выручка компании вырастет на 27,4% в текущем году. Тем не менее фирма испытывает затруднения с выходом на положительную операционную маржинальность уже несколько лет. По результатам 2018 года она составила минус 5,68%. Имея среднюю долговую нагрузку, Palo Alto Networks с трудом ее обслуживает, что ограничивает потенциал роста акций.

Электронная Россия

Как правильно пользоваться госуслугами

Александр Осин,
аналитик управления операций
на российском фондовом рынке
ИК «Фридом Финанс»

Согласно последнему рейтингу BCG, Россия входит в топ-10 стран, население которых активно использует государственные услуги онлайн. Ежемесячно 10 млн человек посещает портал gosuslugi.ru, и это число продолжает расти. При этом уровень проникновения госуслуг среди взрослого населения составляет почти 70%.

Большинство (84%) пока только платит штрафы. По статистике это самая популярная услуга, но востребованы и другие: запись в поликлинику, в ГИБДД, школу или детский сад, оформление загранпаспорта. Их число постоянно растет.

Использование сервисов удаленного обслуживания, как оказалось на практике, несет в себе риски. До недавнего времени считалось, что они низки. Самая распространенная проблема — утрата ключа к электронной цифровой подписи (ЭЦП). Выпуск нового сертификата не занимает много времени, а угрозы, связанные с хищением ключа и сертификата ЭЦП, рассматривались лишь в теории, так как считалось, что никакого практического вреда нанести этой кражей невозможно.

Но ситуация менялась по мере того, как на портал добавлялись новые услуги и он становился все более популярным. Оказалось, что при помощи чужой электронной подписи мошенники могут регистрировать бизнес для ухода от налогов, которые потом госорганы пытаются получить с потерпевшего гражданина.

Официально зафиксирован случай попытки зарегистрировать продажу квартиры не подозревающего об этом собственника при помощи дубликата ЭЦП, полученного мошенническим путем. При этом деньги за проданную недвижимость по договору поступили бы не ее законному владельцу, а злоумышленникам.

Прецедент стал поводом для того, чтобы государство обратило внимание на безопасность организации онлайн-сервиса. В качестве «заплатки» срочно приняли поправки к закону, запрещающие регистрацию прав собственности на недвижимость подачей документов в электронном виде, подписанных ЭЦП, если ранее гражданин не подавал собственноручно соответствующее заявление в Росреестр.

Однако эксперты смотрят на проблему глубже и серьезнее. Получить ЭЦП можно в любом частном удостоверяющем центре, при этом информация о выданных и отозванных сертификатах имеется только у самих центров. Проверить в каком-то одном месте, выдан ли сертификат ЭЦП, и если да, то где и когда — сейчас невозможно. А выдача каждого нового сертификата автоматически не отменяет действие прежнего.

То есть пострадавший узнает о том, что на его имя кто-то выпустил сертификат и пользуется им в преступных целях, только когда негативные последствия уже наступят. И это огромная проблема.

Сначала тревогу забили предприниматели, так как эта схема угрожает бизнесу. С дубликатом ЭЦП лица, имеющего право действовать от имени фирмы, мошенники получают доступ в личный кабинет на сайте ФНС, где могут поправить документы по своему усмотрению. Например, сменить ответственных лиц, перевесить чужую налоговую задолженность и так далее. Потом докажи, что ты ни при чем...

Масштаб угрозы достаточно серьезный, и с появлением дополнительных цифровых сервисов в системе госуслуг будут возникать новые виды мошенничества.

В 2018 году россияне провели через gosuslugi.ru 52 млрд рублей. Наверняка найдутся желающие сделать пару глотков из этого денежного потока.

Как минимизировать риски неправомерного использования ЭЦП:

- Подать заявление в Росреестр о непроведении регистрационных действий без личного присутствия.
- Подать заявление в ИФНС о непроведении регистрационных действий без личного присутствия.
- Отслеживать статус поданных заявлений на портале gosuslugi.ru.
- Бережно хранить сертификат ЭЦП и ключ к нему, принимать меры, предотвращающие их утечку.
- Не использовать простой пароль ключа ЭЦП.
- Отзывать сертификат ЭЦП при его утере или подозрении, что он похищен.

От автокресла до автопилота

Как машины становятся безопаснее и умнее

Артем Чибирев,
старший персональный менеджер
ИК «Фридом Финанс»

С момента появления первого автомобиля в конце XIX века безопасность этого популярного вида транспорта остается актуальной. И хотя человечество далеко продвинулось в способах защиты на дорогах, усложнилась и архитектура дорожного движения, что потребовало новых решений. В борьбу за спокойствие и сохранность пассажиров включились технологические гиганты со своими разработками.

Защита: эволюция

Одной из главных инноваций в сфере безопасности автомобилей стало изобретение, которое отмечает в этом году полувековой юбилей. Столь привычный нам трехточечный ремень был представлен в 1959 году шведской компанией Volvo, а в 1970-1980 годах она среди первых стала разрабатывать детские автокресла и встраивать в авто подушки безопасности.

Со временем к традиционным или механическим системам защиты пассажиров стали добавляться и более «умные». Адаптивный круиз-контроль, который помогает избежать столкновений с впереди идущим автомобилем, слежение за слепыми зонами получают все большее распространение. И если раньше подобные технологии можно было встретить разве что на топовых моделях люксовых брендов вроде Mercedes, то сейчас это не редкость и в более доступных марках.

Экономия на масштабе и растущий спрос позволяют внедрять высокие технологии на все большем количестве рынков, что повышает общий уровень безопасности на дорогах. Например, китайская компания Geely устанавливает опцию 360-градусного обзора в семейный кроссовер Gleagle GX7 в ответ на повышающиеся запросы по безопасности у потребителей.

Технологический прогресс приблизил появление полностью автономного транспорта. Самостоятельное движение автомобилей становится все более безопасным, что приведет к распространению в первую очередь роботакси. Автомобили с технологией автономного движения Waymo от Alphabet только на дорогах Калифорнии проехали более 1,2 млн миль в прошлом году.

Лидерами по разработкам автономных машин являются Waymo, General Motors и Apple, в то время как другие важные игроки вроде Tesla и Uber в него не попали. Дело в том, что Tesla обкатывает свои технологии уже в реальных автомобилях, когда используется функция автопилота. Uber же приостановил испытания после прошлогоднего инцидента с погибшим пешеходом.

Статистика показывает, насколько технологии продвинулись вперед. Причем ради их развития и скорейшего внедрения компании готовы объединяться. К примеру, Waymo кооперируется с основным конкурентом Uber в США, компанией Lyft.

«Яндекс» до конца года также выведет на российские дороги 100 беспилотных автомобилей. Полностью беспилотный и безопасный транспорт, по плану компании, должен быть запущен до марта 2021-го.

Китайские гиганты вроде Baidu или Tencent также активно участвуют в гонке технологий.

Производители автономного транспорта

Источник: Департамент транспортных средств Калифорнии

Минус человек

Последняя буква в аббревиатуре ДТП означает происшествие, то есть случайное событие. Автономные автомобили же сделают эти несчастные случаи ошибкой, которую можно устранить. По данным McKinsey, автономные машины способны сократить число смертей по причине вождения на 90%. Для сравнения, только в США это почти 300 тысяч жизней за 10 лет.

Беспилотные технологии могут стать революционным новшеством в области автобезопасности — как когда-то им стали ремни, подушки и детские кресла.

Как в мире изменились траты на военную промышленность в 1988–2018 гг.


Россия
3,9% ВВП
Европа
603
млн $
348
млн $
-42%
Азия
494
млн $
134
млн $
+268%
Африка
39,2
млн $
16,4
млн $
+39%
Китай
1,9% ВВП
Индия
2,4% ВВП
ЮАР
1,0% ВВП

Доходные отходы

Как превратить мусор в источник прибыли

Рональд Вусик,
заместитель директора
департамента по работе с клиентами
ИК «Фридом Финанс»

Традиционно расходы на экологию в мире считались исключительно дотируемой сферой. Государства выделяли на нее немалые деньги, а окупаемость таких трат была весьма относительной.

Многое изменилось с развитием технологий, однако суть большинства экологических проектов остается прежней: они спонсируются из бюджетов разного уровня, через экологические налоги с предприятий и так далее. Но это тоже бизнес, так как вокруг сфер, для которых искусственно создают тепличные условия, образуются специализированные компании, готовые на этом зарабатывать. Некоторые из них существуют десятилетиями и давно стали публичными. Разумеется, самые крупные из них работают в США.

Давайте с ними познакомимся.

Мусор Нового Света

Крупнейшей публичной компанией Соединенных Штатов, которая превращает мусор в выручку, является Waste Management Inc. Ее акции торгуются на бирже NYSE под тикером WM.

Компания — ведущий поставщик услуг по сбору и захоронению отходов. В 2018 году она отправила 117 тысяч тонн мусора на свои 252 полигона, а капитальные инвестиции в переработку превышают $1 млрд.

Waste Management стремится поддерживать высокие экологические стандарты ведения бизнеса — 6500 ее грузовиков работают на природном газе. Также она занимается глубокой переработкой мусора и генерацией электроэнергии из производимого биотоплива. Компания построила первый в мире коммерческий биоперерабатывающий завод, продукцией которого стало биотопливо: метанол и этанол.

Совокупная выручка от обслуживания более 20 млн клиентов составляет не меньше $15 млрд в год. Денег хватает на покупку конкурентов. Например, в апреле стало известно, что компания поглотит Advanced Disposal Services (ADSW) за $5 млрд.

Основной визави WM — фирма из Аризоны Republic Services. Тоже, кстати, публичная: ее акции торгуются на NYSE под тикером RSG. Компания управляет 64 центрами утильсырья по всем Соединенным Штатам, перерабатывая 2,5 млн тонн мусора ежегодно. В августе 2017 года RSG заявила о покупке крупного оператора по сортировке и переработке бытового мусора ReCommunity Holdings.

С момента выхода на IPO в 1998 году акции Republic Services выросли в пять раз. Биржевая стоимость компании составляет $28 млрд. Согласно данным сервиса Yahoo.Finance, аналитики крупных инвестдомов советуют держать и покупать эту бумагу.

Еще одним заметным игроком из этой сферы является канадская GFL Environmental, которая собирается провести IPO на фондовой бирже Торонто в сентябре. Компания планирует продать свои акции на $1,5 млрд при оценке всего бизнеса в $15 млрд. По данным Bloomberg, это размещение станет крупнейшим в Канаде за последние 5 лет. GFL Environmental имеет собственные мощности в Канаде и США, обслуживающие 4 млн домохозяйств и 135 тысяч корпоративных клиентов. Компания занимается вывозом твердых отходов, восстановлением почв и переработкой жидких отходов для повторного использования — в основном это масла, масляные фильтры, антифриз, отработанные гликоли, растворители, абсорбенты, жидкости для химической чистки, смазочные материалы и легкие виды топлива. Штат насчитывает 9500 сотрудников.

Компания активно растет, в основном покупая более мелких игроков и заключая долгосрочные контракты на вывоз и переработку мусора. За счет этого удалось нарастить выручку до $2,24 млрд за последние 12 месяцев.

Кроме уже упомянутых компаний сферы утилизации отходов, публичными являются еще 22 предприятия: Stericycle (тикер SRCL), Waste Connections (WCN), U.S. Ecology (ECOL) и другие. Их суммарная капитализация превышает $120 млрд. Большинство из них прибыльны, а стоимость акций всех компаний из первой десятки сектора переработки отходов США выросла с начала года.

Источник: shutterstock.com

Весь сор в одной избе

Для желающих заработать не на конкретных предприятиях, а на всей индустрии отходов на Уолл-стрит есть подходящий продукт — биржевой инвестиционный фонд VanEck Vectors Environmental Services ETF. Он появился в 2006 году и 13 лет подряд приносил своим инвесторам в среднем 8,85% годовых в долларах.

В портфель этого фонда входят акции 23 американских компаний. В тройке крупнейших вложений, помимо Waste Management и Republic Services, производитель дезинфекционного и стерилизационного оборудования Steris.

Фонд торгуется на бирже NYSE Arca под обозначением EVX. На момент написания статьи стоимость одной его акции составляла порядка $100. Как и любой другой инвестиционный фонд, EVX взимает ежегодную комиссию за управление в размере 0,98%.

Несмотря на небольшой размер активов под управлением ($36,5 млн) и более высокие комиссионные, чем в среднем по индустрии ETF, фонд EVX способен занять достойное место в портфеле борца за экологию.

Чистая Поднебесная

Возможность заработать на экологии есть не только у инвесторов в американские активы. В конце июня агентство Bloomberg обратило внимание на стремительный рост акций китайских компаний, занимающихся переработкой мусора. Их бумаги торгуются на Шанхайской и Шэньчжэньской фондовых биржах.

Инвесторы стали скупать акции оператора пищевых отходов WELLE Environmental, производителя мусоровозов Fujian Longma Environmental Sanitation Equipment и переработчика отходов Tus-Sound Environmental Resources, подбросив цену на десятки процентов за несколько дней.

Поводом для роста стало заявление китайского Министерства жилищного строительства и развития городских и сельских районов. Ведомство заявило о старте программы по внедрению раздельного сбора мусора в 46 крупнейших городах страны к 2020 году. И хотя эксперты ждут большей конкретики в части ее реализации на местах, инвесторы и спекулянты уже увидели в самом факте ее наличия возможность заработать на потенциальном росте спроса на продукцию этих компаний.

Чистое будущее

Забота об окружающей среде — часть менталитета миллениалов, образа жизни сотен миллионов молодых людей по всему миру. Насколько та или иная компания заботится об окружающей среде, перешла ли она на новые экологические стандарты производства — эти вопросы будут волновать их не меньше, чем финансовые показатели бизнеса.

Здоровье в режиме онлайн

Кто зарабатывает на стремлении людей знать все о своем теле

Евгений Миронюк,
аналитик
ИК «Фридом Финанс»

Сегодня здоровый образ жизни — это не только постоянные тренировки и правильное питание, но и сбор и анализ показателей здоровья человека в режиме реального времени.

Трендом последних 10 лет стало распространение гаджетов, помогающих фиксировать результаты занятия спортом, в частности трекеров и фитнес-браслетов. Они помогают четко нормировать нагрузку и следовать программам тренировок. Ведь важно не только достичь поставленных целей, но и не сорвать мышцы, не получить травму.

Важнейшим фактором стала мотивация пользователя. Привязанность к достигнутым показателям и желание их улучшить на основе четких количественных изменений заставляют производителей предлагать больше функций в устройствах, а пользователей — чаще обновлять свои гаджеты. Профессиональным спортсменам такие устройства необходимы как воздух, так как они собирают информацию обо всех тренировках, состоянии организма и окружающей среды.

Источник: shutterstock.com

Глобальная слежка

Производителей, специализирующихся исключительно на изготовлении подобной микроэлектроники, не так много. Рынок захватили известные и крупные международные бренды: Apple, Xiaomi, Sony, Huawei, Microsoft. Но есть и ветераны индустрии, которые успешно борются с гигантами электроники за право считаться производителем лучшего устройства для анализа здоровья.

К ним относится американская компания Fitbit Inc. (NYSE: FIT), основанная в Сан-Франциско в 2007 году. Несмотря на то, что финансовые показатели компании далеки от своего пика, капитализация бизнеса превышает $1 млрд.

Производителем профессиональных трекеров является международная фирма Garmin (NASDAQ: GRMN). В начале своего пути компания специализировалась на технологии GPS, интегрировании ее в автомобильные, авиационные и морские приборы. Популярный бренд компании — навигатор eTrex. Это одна из первых зарубежных компаний, которая стала предлагать навигацию на основе российской навигационной системы ГЛОНАСС.

Но ниша товаров для спорта оказалась для Garmin не менее выгодной. В фитнес-браслетах этой компании используется программа «личный тренер», учитывающая индивидуальные особенности спортсмена. Особенно они полюбились триатлетам, которым важно отслеживать пульс и другие показатели во время преодоления длинных дистанций.

Выручка компании в период с 2009 по 2018 год росла незначительными темпами и достигла $3,34 млрд по итогам 2018-го, данные первых двух кварталов 2019-го указывают на существенный рост продаж (г/г). Доля приборов для автомобильной навигации в общем объеме продаж компании за эти годы уменьшилась с 70 до 19%, уступив фитнес-браслетам (26%) и другим носимым устройствам (24%). Это позволило нарастить валовую прибыль с $1,4 млрд в 2009 г. почти до $2 млрд

в 2018 г. В настоящий момент капитализация компании превышает $16 млрд, с начала года она выросла более чем на 40%.

Наибольшего прогресса достигла компания Apple (NASDAQ: AAPL), превратившая свои наручные часы Apple Watch в многофункциональное устройство с внедренными в него самыми передовыми технологиями миниатюризации. Устройство не просто измеряет сердечный ритм, но и фиксирует отклонения, выдает рекомендации для посещения врача-специалиста. Например, предварительно диагностирует фибрилляцию предсердий.

Эта технология заинтересует людей, предрасположенных к сердечным заболеваниям, а также тех, кому требуется нормировать физическую нагрузку. Также Apple Watch отслеживает другой важный показатель — качество сна.

Попытки создания неинвазивных датчиков, определяющих уровень сахара в крови, глюкометров, ведутся уже давно. Количество людей с сахарным диабетом в мире растет, но до сих пор не удавалось сделать эти устройства по-настоящему мобильными. Группа биомедицинских разработчиков Apple работала над этим с 2010 года, новинка анонсирована и должна появиться в ближайшее время.

До этого портативные глюкометры брали анализ крови, прокалывая палец. Технология Apple, использующая оптические датчики, действующие через кожу, имеет все шансы стать прорывной. Американское Управление по контролю за качеством пищевых продуктов и лекарственных препаратов (FDA) запустило пилотную программу по предварительной сертификации компаний, занимающихся разработкой портативных устройств и приложений для медицинских нужд. Apple стала ее участником. Ожидается, что среднегодовой рост этого рынка составит 18% вплоть до 2024 года.

Модная защита

Из публичных компаний, производящих качественную спортивную защиту, отметим немецкую Adidas (FWB: ADS). Компания предлагает шлемы, наколенники, налокотники, напульсники, защиту голени. Помимо надежной защиты бренд отличает строгий и при этом функциональный дизайн.

В 2006 году в состав компании влился всемирно известный спортивный бренд Reebok, в линейке товаров которого также немалое внимание уделено спортивной защите. 2019 год удачен для компании в том числе за счет вывода на рынок высокотехнологичных новинок в сегментах одежды и обуви. Рыночная капитализация выросла на 50% с начала года.

Рост благосостояния среднего класса позволяет выделять все больше денег на товары и услуги, помогающие вести здоровый образ жизни. По оценке FDA, только рынок носимых медицинских устройств превысит $14 млрд к 2024 году.

Стремительное проникновение «умных» гаджетов в массовый потребительский сектор может в разы повысить спрос на трекеры и фитнес-браслеты, которые найдут себе место на рынке, несмотря на наличие подобных функций в «умных» часах и смартфонах. Коммерциализация массового спорта сделает и элементы защиты неотъемлемым аксессуаром при покупке спортивных товаров.

Источник: shutterstock.com

Ставка на осень

К старту делового сезона мы подобрали компании из разных отраслей зарубежной и российской экономики, которые могут порадовать инвесторов хорошей доходностью до конца года

Илья Атамановский,
старший
персональный менеджер
ИК «Фридом Финанс»

LOCKHEED MARTIN

Целевая цена:

$411

Потенциал роста:

7%

Lockheed Martin обслуживает оборонную промышленность Соединенных Штатов и работает на экспорт. Компания поддерживает стабильный уровень рентабельности производства в последние годы, возврат на капитал (ROE) выше 100%. Одно из слабых мест — серьезная долговая нагрузка по отношению к активам и акционерному капиталу. Причина в программе выкупа акций, которая сокращает акционерный капитал на бухгалтерском балансе фирмы. Позитивный фактор — высокий спрос на истребители F-35, дающие 27,5% выручки.

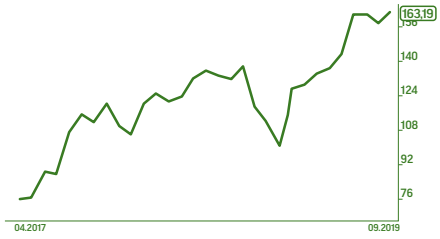
Ferrari

Целевая цена:

$174

Потенциал роста:

10,3%



Благодаря премиальному сегменту бизнес Ferrari имеет высокую операционную маржинальность на уровне 20% за последние 4 года против 4% у General Motors и 3% у Ford. Выручка компании также растет быстрее конкурентов, и этот рост менее подвержен циклическим спадам, так как спрос на люксовые товары даже в кризис остается высоким. По результатам II квартала повышен прогноз по чистому денежному потоку на год с €0,45 млрд до 0,55 млрд. Благодаря программе выкупа акций на $1,2 млрд и дивидендной доходности акций в районе 2,64% бумаги Ferrari способны продолжить уверенный рост.

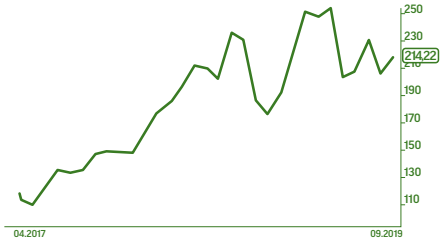
paloalto NETWORKS

Целевая цена:

$236

Потенциал роста:

15,9%



Компания разрабатывает системы кибербезопасности. Выручка растет на 20-30% в год, но при этом бизнес имеет отрицательную операционную маржинальность, которая вынуждает менеджмент брать кредиты. Для укрепления лидирующих позиций на рынке Palo Alto Networks активно расширяется, поглощая малые компании в лице Demisto, RedLock, CyberSecdo и Evident.io. Ожидается, что с 2018 по 2021 год выручка вырастет с $2,3 до 4 млрд.

GENERAL DYNAMICS

Целевая цена:

$219

Потенциал роста:

15,2%

General Dynamics имеет высокую долговую нагрузку и низкие коэффициенты ликвидности. Тем не менее она легко обслуживает долги благодаря росту продаж и рентабельности чистого дохода на уровне 11%. Фирма выкупает свои акции с рынка на $1,2 млрд и выплачивает дивиденд на уровне 2,14% годовых. По результатам второго квартала менеджмент повысил прогноз по выручке и операционному доходу за год.

Арсений Цванг,
заместитель директора
департамента продаж
ИК «Фридом Финанс»

ЛЕНТА

Целевая цена:

228,33 ₽

Потенциал роста:

4,83%

Убыток ПАО «Лента» по итогам I полугодия — разовое явление. Мы ожидаем увидеть чистую прибыль уже во II полугодии. Планируемая регистрация компании в качестве налогового резидента РФ повысит ее инвестиционную привлекательность. После периода неопределенности возможен рост спроса на бумаги «Ленты».

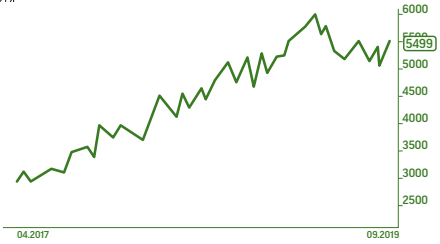
ЛУКОЙЛ
НЕФТЯНАЯ КОМПАНИЯ

Целевая цена:

5927 ₽

Потенциал роста:

9,6%



ПАО «ЛУКОЙЛ» в очередной раз продемонстрировало свою заботу об акционерах. Компания вовремя сократила инвестиционные расходы в условиях рисков для прибыли, возникших из-за повышения налогов и нестабильности рублевых цен на нефть. Это оказало решающее влияние на формирование позитивной финансовой отчетности компании. Кратко- и среднесрочный драйвер роста — продолжение стратегии выкупа «ЛУКОЙЛом» своих акций с открытого рынка.

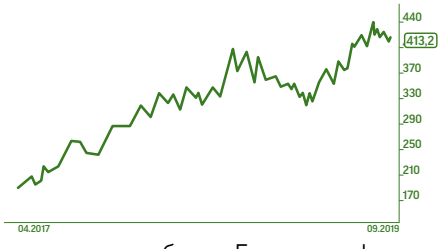
ГАЗПРОМ НЕФТЬ

Целевая цена:

476 ₽

Потенциал роста:

12,5%



За счет роста добычи чистая прибыль «Газпром нефти» в I полугодии выросла на 29,2% год к году. Совет директоров компании рекомендовал выплатить дивиденды за январь-июнь объемом 18,14 рубля на акцию. Общий объем выплат составляет 40% чистой прибыли по МСФО (в прошлом году — 37,8%). В июне 2019-го сообщалось, что «Газпром нефть» ставит целью поднять дивиденды до 50% от чистой прибыли по МСФО в среднесрочной перспективе.

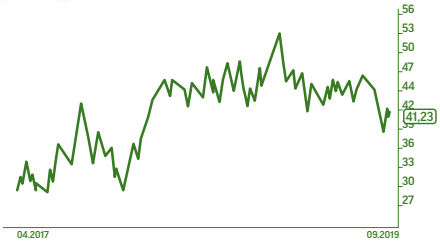
МАГНИТОГОРСКИЙ МЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ

Целевая цена:

50 ₽

Потенциал роста:

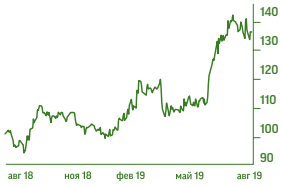
21,5%



В августе появилась информация о том что в сентябре будет внесена в правительство на рассмотрение программа развития угольной отрасли. Эта новость подкрепляет ожидания инвесторов о комплексной централизованной поддержке металлургии и добычи, которая была ранее обозначена введением Европейской экономической комиссией ограничений на импорт труб большого диаметра с 1 декабря 2019 года.

Ерлан Абдикаримов
Директор Департамента аналитики
ИК «Фридом Финанс»

Тикер: **HSBK**
Текущая цена: **129 тг**
Целевая цена: **142 тг**
Потенциал роста: **10%**



«Народный сберегательный банк Казахстана» является крупнейшим банком Казахстана и занимает долю в 34,4% в банковском секторе (у ближайшего конкурента - 7,8%) по размеру активов. Кроме банковской деятельности, группа «Halyk» также занимается страховой, брокерской и лизинговой деятельностью. Деятельность группы также осуществляется в Кыргызстане, Греции, России и в Узбекистане. После приобретения «Казком» на условиях вывода проблемных активов государством Народный банк значительно улучшил свои позиции на рынке. Благодаря синергии и удалению дублирующих функций двух банков Группа сумела значительно сократить операционные расходы и нарастить прибыль до рекордных для себя размеров. Также Группа изменила дивидендную политику, увеличив долю чистой прибыли, направляемую на дивиденды, с 0-50% до 50-100%. На фоне почти двукратного роста чистой прибыли (14,06 тенге на акцию за первое полугодие) акции Группы могут стать интересным дивидендным вариантом с хорошей доходностью. Мы прогнозируем, что дивиденды могут составить от 14 до 28 тенге на акцию по итогам 2019 года, что дает дивидендную доходность в 11-22% от текущих цен.

Тикер: **KZTO**
Текущая цена: **993 тг**
Целевая цена: **1 200тг**
Потенциал роста: **21%**

«КазТрансОйл» — национальный оператор Казахстана по магистральному нефтепроводу. Компания располагает сетью магистральных нефтепроводов протяженностью 5 378 км и водоводов протяженностью 1 945 км. Также компания оказывает услуги по обслуживанию трубопроводов, перевалки, экспедиции и хранения нефти. Компания имеет дочерние предприятия в Грузии и владеет морским нефтяным терминалом в Батуми. Компания осуществляет транспортировку нефти как на экспорт в Самару и в Китай, так и на внутренний рынок, поставляя сырую нефть на три нефтеперерабатывающих завода и битумный завод. Кроме того, «КазТрансОйл» занимается транзитом российской нефти из Омска в Китай и в Узбекистан. Несмотря на падение дивидендов в 2018 году, отчет за первое полугодие 2019 года указывает на возможное возвращение чистой прибыли на уровень 2017 года, что предполагает дивиденды в размере 150-160 тенге на акцию в случае отсутствия шоков на валютном рынке до конца года, которые и стали причиной падения чистой прибыли в прошлом году. В случае исполнения данного сценария дивидендная доходность акции может составить 15-16% от текущих цен.

Тикер: **KAP**
Текущая цена: **5 659 тг**
Целевая цена: **6 200 тг**
Потенциал роста: **9,5%**

«Казатомпром» является самым крупным производителем урановой продукции в мире, на долю которого приходится около 20% мирового производства урана. Запасы урана компании составляют свыше 300 тыс. тонн. Все урановые активы компании являются геологически уникальными и разрабатываются методом подземного скважинного выщелачивания, за счет чего компания имеет один из самых низких показателей себестоимости производства. Также компания производит такие редкие металлы, как бериллий, тантал, ниобий, топливные таблетки. В конце августа «Казатомпром» отчитался за первое полугодие 2019 года. Отчет оказался умеренно позитивным благодаря росту выручки на 22%, который охватил девальвацию тенге к доллару, и росту скорректированной чистой прибыли почти в 2,5 раза. Отмечаем рост операционного денежного потока до 111,4 млрд тенге, что может стать подспорьем для выплаты дивидендов по итогам этого года.

Тикер: **GB_KZMS**
Текущая цена: **2 235 тг**
Целевая цена: **2 710 тг**
Потенциал роста: **21%**

KAZ Minerals PLC — международная компания по добыче природных ресурсов, работающая в Казахстане и соседнем регионе. Занимается производством и продажей меди. Осуществляет полный цикл работ от добычи руды до производства готового металла. Мededобывающее подразделение занимается производством металлов, являющихся побочными продуктами производства, включая цинк, серебро и золото. В связи с тем, что выручка компании номинирована в долларах, она может выиграть в случае ослабления тенге к доллару. По моему мнению, недавнее падение цен акций KAZ Minerals после отчета за первое полугодие оказалось эмоциональным, и фундаментально компания должна стоить выше как по отношению к аналогам на рынке, так и относительно финансовых показателей. В техническом плане цены могут показать разворот в случае пробития уровня сопротивления в 2 150 тенге на акцию.

Вместо стеклянной банки

Мировой рынок сейфов растет за счет роста благосостояния жителей азиатского региона. Теперь им есть что прятать за железной дверцей. На чью продукцию ожидать повышенный спрос?

Максим Леушкин,
старший
персональный менеджер
ИК «Фридом Финанс»

Сегодня мировой рынок сейфов и хранилищ оценивается в $5,3 млрд, а к 2025 году, по нашим расчетам, он подрастет до $7,1 млрд, увеличиваясь в среднем на 5% в год.
Основной спрос на сейфы формируется в Азиатско-Тихоокеанском регионе из-за экономического роста входящих в него стран. Также производящие их компании смогут заработать и в Северной Америке, но уже на продаже оружейных сейфов — как известно, по закону граждане США имеют право покупать и хранить у себя в доме чуть ли не целый арсенал разнокалиберных пушек.
Крупнейшими компаниями на рынке устройств хранения ценных и опасных вещей являются Godrej & Boyce Manufacturing, FireKing Security, American Security (AmSec), Gardall Safe, HAYMAN Safe, Hollon Safe, Mesa Safe, Mutual Safe, Alpha Safe & Vault, Diebold Nixford и Gunnebo Group. Однако из них на бирже торгуются только две. Обсудим их перспективы.

Gunnebo Group (тикер GUNN). Шведская компания — мировой поставщиком продуктов, услуг и программ для обеспечения безопасности. Gunnebo защищает банки, магазины розничной торговли, общественный транспорт, общественные и коммерческие здания, а также промышленные и объекты повышенной опасности.
Линейка продуктов включает огнеупорные и взломоустойчивые сейфы и шкафы, банковское оборудование (традиционные и автоматические системы депозитных ячеек), сейфовые хранилища, двери для сейфовых хранилищ и т. д. Одним из наиболее интересных продуктов компании является система OneID, заменяющая паспортный контроль в аэропортах. Она позволяет сэкономить время и ресурсы, увеличив эффективность работы аэропорта.
Корпорация владеет такими брендами, как Gunnebo, Chubbsafes, Steelage, Hamilton и т. д. Также в начале июля Gunnebo Group приобрела чешскую компанию Cominfo, предлагающую решения для систем контроля доступа.

Рыночная капитализация на бирже Nasdaq Nordic составляет порядка 1,992 млрд шведских крон, или около $211 млн. Последний год акции Gunnebo Group торгуются в диапазоне от 21,45 до 31,25 кроны ($2,27-3,31). Коэффициент цена/прибыль (P/E) находится в районе 18,75, прибыль на акцию (EPS) равна 1,36. Рост выручки с 2017 по 2018 год составляет 5,49%.

Diebold Nixdorf (DBD). Производитель комплексных систем самообслуживания и безопасности для банков и финансовых институтов. Сюда входят банкоматы, хранилища, сейфы, управление замками и ключами, программное обеспечение и так далее.
Каждый третий банкомат в мире произведен именно этой компанией. Из интересных продуктов Diebold Nixdorf упомянем новую серию банкоматов самообслуживания, которые могут поддерживать цифровые функции, такие как биометрия и NFC.
Компания размещена на Нью-Йоркской бирже NYSE, рыночная капитализация составляет $925 млн. Акциям еще далеко до исторических максимумов в $58, которые были достигнуты в далеком 2003 году. Однако, согласно сервису Yahoo.Finance, аналитики рекомендуют держать и покупать Diebold Nixdorf, целевая цена — $12,5 за бумагу.

Рынок сейфов 2016 года — конечные потребители (внебанковский сектор)

Источник: safe4you.ru

Деньги в безопасности

По просьбе «Финансиста» российские эксперты в области информационной безопасности рассказали о том, как их компании защищаются от различных видов угроз, а также выделили перспективные акции для вложений в этот сектор

Вячеслав Касимов,
директор департамента информационной безопасности Московского кредитного банка

Сегодня мы рассматриваем четыре основные группы угроз. Во-первых, угрозы, связанные с атаками непосредственно на банк, когда злоумышленники ищут платежные системы или шлюзы и стараются либо добавить туда платежи, либо модифицировать уже существующие. Во-вторых, атаки на клиентов банка: получение доступа к личным кабинетам при дистанционном банковском обслуживании, совершение переводов с карты на карту. В-третьих, атаки на банкоматы и терминалы для приема денег. И в-четвертых, разглашение клиентских данных.

В нашем банке сформирована стратегия информационной безопасности, в которой вышеназванные угрозы являются одними из важнейших компонентов. Кроме того, в ней заложены принципы нулевой толерантности к мошенничествам, четкого исполнения нормативных и регуляторных требований, а также принцип «запрещено запрещать». Если мы видим, что бизнес или IT хочет внедрить полезное решение или продукт, но сама реализация не выглядит безопасной, тогда мы просто предлагаем альтернативный механизм реализации.

Денис Масленников,
эксперт Аналитического центра Санкт-Петербургской биржи

Американские компании, связанные с кибербезопасностью, относятся к подотраслевой группе Systems Software. Туда входят Symantec Corp, известная благодаря одноименному антивирусу, Cyberark Software, занимающаяся разработкой систем цифровой защиты для финансового сектора и госструктур, а также Proofpoint.

Акции компаний информационной безопасности подходят для инвестиций благодаря большой отдаче на капитал: этот тип бизнеса легко масштабируется и не требует значительных затрат для расширения. Например, средняя отдача капитальных вложений Symantec Corp за пять лет составила 276%. На данный момент эта акция интересна еще в связи с недавно объявленной сделкой по поглощению компании со стороны Broadcom.

Дмитрий Кузеванов,
руководитель отдела информационной безопасности сети супермаркетов «Азбука вкуса»

Все более высокий уровень цифровизации ритейла приводит к тому, что возможной целью для хакерских атак становится инфраструктура магазинов, например кассы, терминалы сбора данных, сетевое оборудование и прочее. Любая из систем этих устройств может стать «нулевым пациентом», а с учетом растущей комплексности и сложности угроз это открывает новые опасные векторы атаки.

Применение SDL (жизненного цикла безопасной разработки) в компании помогает решить широкий спектр проблем — от уменьшения стоимости исправления возможных ошибок (включая отказы и корректировки задач на этапе формирования идеи) до обучения персонала во время выполнения им своих задач (например, консультаций по архитектурному решению). А внедрение SOC (центра оперативного управления информационной безопасностью) помогает контролировать поток событий в сфере информационной безопасности. Только оперативное, полноценное и всестороннее понимание проблем помогает качественно их устранять.

С учетом роста количества переносимых устройств, их активной интеграции в корпоративную инфраструктуру, а также растущей сложности методов социальной инженерии эффективный подход к обучению персонала в области информационных технологий и информационной безопасности будет являться вызовом в недалеком будущем. Изменения в IT приходят очень быстро, нужно уметь гибко и быстро обучать персонал с учетом этих изменений.

Ольга Лоншакова,
руководитель отдела продаж и развития рынка PayPal в России и странах Балтии

Сегодня купить, продать или перевести деньги в другую точку планеты можно даже не включая компьютер — с телефона в дороге, на беговой дорожке или родительском собрании. Чем больше эта сфера, тем интереснее она для злоумышленников и тем важнее всегда оставаться на шаг впереди них. Доверие и безопасность становятся ключевыми. Для PayPal эти понятия — ДНК бизнеса. Мы обрабатываем 27 млн транзакций в день. Используя эти знания, помимо прочего, строим защитные механизмы, которые совершенствуются с каждым переводом. За пару секунд, пока идет оплата покупки, на нашей стороне проходит от сотен до нескольких тысяч специальных проверок — чтобы при привычной пользователю скорости и простоте обеспечить максимальную безопасность.

Сергей Демидов,
директор департамента операционных рисков, информационной безопасности и непрерывности бизнеса Московской биржи

Главная задача Московской биржи — бесперебойность биржевых торгов, предоставление инвестору возможности в любой момент купить или продать актив — будь то акция, облигация или валюта. Это обеспечивается самыми современными средствами и значительными инвестициями в IT-технологии и технологии обеспечения безопасности, мы используем очень широкий спектр решений от разных поставщиков на разных технологических участках.

Доступ к биржевой инфраструктуре имеют различные типы организаций — от банков и брокеров до компаний реального сектора экономики, с которыми биржа взаимодействует по специальным каналам связи и протоколам обмена информацией. Биржевые системы расположены в максимально защищенных и надежных дата-центрах. Торговая система биржи и все ресурсы биржи, доступные извне, регулярно проходят самые сложные проверки с точки зрения безопасности и доступности. Таким же проверкам подвергаются и сами системы безопасности.

Безусловно, системы безопасности будут эволюционировать, все больше средств защиты будут включать в себя элементы искусственного интеллекта и машинного обучения. Мы видим будущее информационной безопасности во многом как партнера с IT и бизнесом, помощника в реализации задач любого уровня сложности.

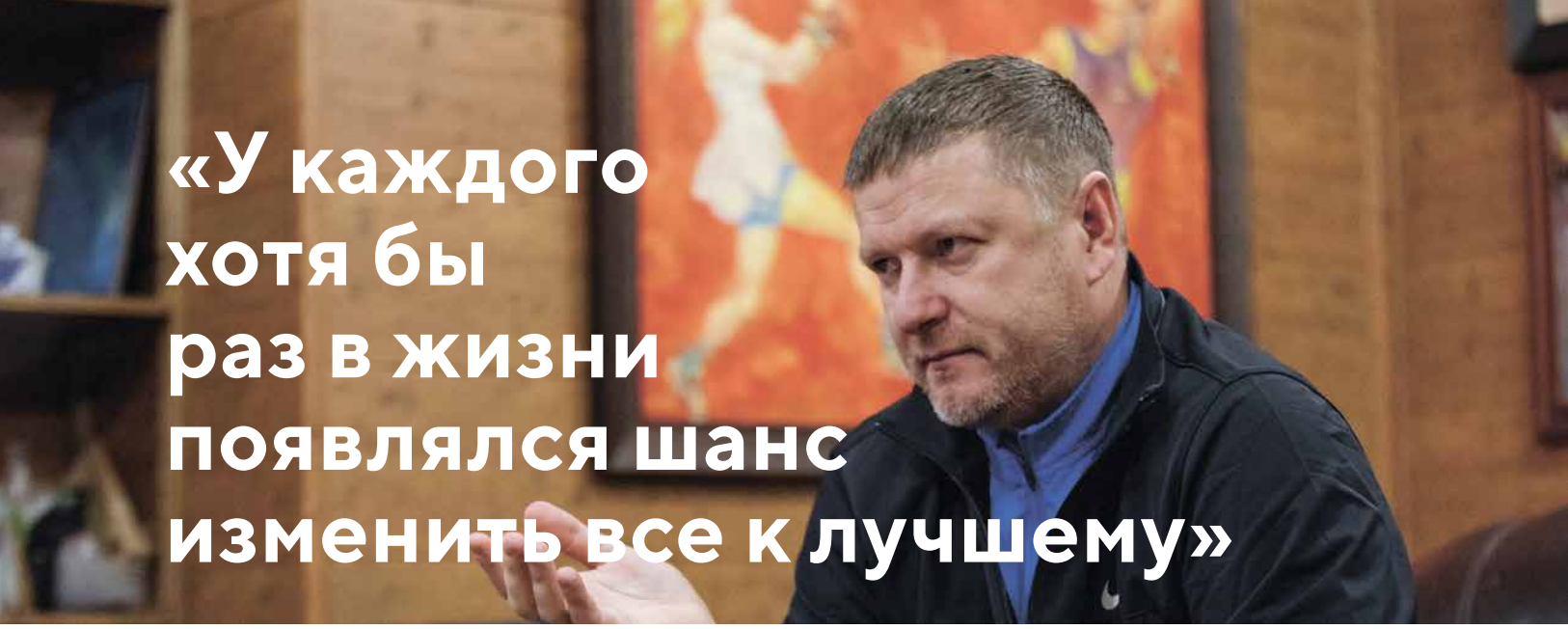
Дмитрий Найденов,
директор по информационной безопасности S7 Group

Как показывают последние события, произошедшие в крупных международных компаниях, таких как British Airways, Marriott, Alphabet, Facebook, утечка персональных данных может привести к существенным репутационным и финансовым потерям. Появляются новые угрозы, связанные с облачными вычислениями, микросервисной архитектурой, системами контейнеризации, технологиями искусственного интеллекта и тому подобные, которые не могут быть нивелированы существующими подходами как с технической, так и с юридической стороны. Средства защиты и противодействия не успевают за новыми угрозами, поэтому нам приходится адаптировать текущие и разрабатывать собственные технологии защиты, при этом довольно часто используя решения Open Source. Естественно, мы не забываем и про адаптацию наших процессов под изменяющиеся требования законодательства, как отечественного, так и иностранного — я имею в виду GDPR и иные регуляционные нормы и правила.

Юлия Горелова,
директор департамента развития платежного бизнеса «Яндекс.Касса»

Привлечение новых клиентов — главный вызов для компаний, которые ведут бизнес в интернете, показывает недавнее исследование «Яндекс. Кассы» и РАЭК. Для решения этой проблемы бизнес использует маркетинговые инструменты, в том числе бонусные программы. Однако чем больше интересных акций запускают компании, тем более активными становятся мошенники, зарабатывающие на них.

Поэтому онлайн-безопасность — не менее важная проблема наших дней. «Яндекс.Касса» уже дала ответ на этот вызов и разработала антифрод-систему, которая помогает компаниям защититься от накрутки бонусов и таким образом экономить заметную долю маркетингового бюджета. При этом в глобальном мире, где крупные компании работают и за пределами своей страны, система настройки антифрода должна быть максимально гибкой, чтобы не терять клиентов, если их профиль отличается от типичного для вашего локального рынка.



«У каждого хотя бы раз в жизни появлялся шанс изменить все к лучшему»

Теннисист Евгений Кафельников — о деньгах и жизни

Евгений, расскажите о первом серьезном заработке.
Как и все, кто хочет стать профессиональным теннисистом, я начинал карьеру с участия в «сателлитах» — турнирах самого низкого уровня с мизерным призовым фондом. За победу давали полторы тысячи долларов. В одном из них я, кажется, дошел до четвертьфинала и заработал первые призовые — $350.
Шел 1992 год, мне 18 лет. Тогда это была серьезная сумма, ведь у меня не было денег на выезд за границу, я себя не обеспечивал, тренеру платить не мог и так далее. Однако на меня вышла хорошая американская фирма IMG, которая представляет интересы многих спортсменов и мировых звезд, и открыла мне кредитную линию, чтобы я мог покрывать свои расходы.
Вернул им деньги в первой половине 1993 года — порядка $75 тысяч. После этого стал понимать, сколько зарабатываю и на что трачу.

Кто помогал правильно распоряжаться деньгами, когда их стало много?
Я подписал с IMG долгосрочный контракт, они занимались моими финансами до окончания спортивной карьеры. Меня курировали два финансиста, которые постоянно звонили, спрашивали, консультировали. «Нужно сделать инвестиции сюда, ты не против?» — «Да, вы занимайтесь, ради бога. Я не эксперт в этом. Я вам доверяю».
Не было прецедента, чтобы они потеряли мои деньги.

Во что вкладывали?
Я был молодой человек довольно консервативного плана, не любил авантюрные вложения с потенциальным заработком 30-40% годовых. Для меня было комфортно получать свои 1-3% годовых в банке, но зато стабильно. Я знал, что в любой момент, если мне что-то понадобится, смогу ими воспользоваться без проблем. Для меня это было очень важно.

Консультанты ограждали от мошенников?
Нет, от мошенников никак не оградишься. Естественно, вокруг меня болтались какие-то шарлатаны. Не скрою, что даже пострадал от них. Одалживал людям, которые потом не возвращали. Если прикинуть, то у меня невозвратных должников по миру бегает не на один миллион.

В одном из интервью вы признались, что у вас есть неудачный опыт инвестиций на бирже во времена краха доткомов. Можете о нем рассказать?
В 1998-1999 году был настоящий биржевой бум интернет-компаний. Люди покупали акции и обогащались, как у нас в 2000-е на вложениях в недвижимость. Грубо говоря, инвестируешь $100 тысяч, а через 2-3 года становишься мультимиллионером. Тогда акции, стоившие $0,1, взлетали до $400. Представляете, что это такое!
Спортсмены между собой общаются, кто-то рассказал о своих успехах, и я решил попробовать. Открыл брокерский счет в немецком банке и начал активно торговать. Сперва внес $100 тысяч, потом довел счет до нескольких миллионов долларов. В какой-то момент на бирже крутилось до 25% всех заработанных денег за карьеру.

Какие акции запомнили?
Qualcomm хорошо помню. Особенно когда эта акция сначала стоила $400, а потом $10. Но на самом деле я больше торговал опционами, а не бумагами.
Доходило до абсурда: по 5-6 раз в день звонил брокеру и отдавал приказы покупать-продавать. Я на самом деле потерял немалую сумму на бирже, но, слава богу, вовремя остановился и все вывел.

В чем видите причину неудачного опыта? Страх, жадность?
Наверняка это жадность. Что еще может двигать людьми, когда они не могут остановиться? У меня много дру-

зей почему-то решили, что биткоин с $20 тысяч пойдет на $50 тысяч. Я им говорил: «Остановитесь, это все виртуальное!» Им же казалось, что рост продолжится и дальше, но вы сами видите, что с ним происходит.
Сам я в биткоин не вкладывался — не верю в эту пирамиду. Мое жизненное кредо: лучше синица в руке, чем журавль в небе. Это 100%.

Неудивительно, что в какой-то момент вы решили инвестировать свое состояние в недвижимость. Как это произошло?
Ничего особенного — мне предложили пару офисных объектов, спросили: «Берешь или нет?!». Вложился — и с тех пор получаю небольшой доход. Вообще мои доходы, не буду лукавить, упали на 70% в связи с кризисом, санкциями, ослаблением рубля. Конечно, это не то комфортное состояние, в котором бы мне хотелось быть. Тяжело, но держусь.

Какую доходность дает ваша недвижимость? 6-7%?
Нет, сейчас меньше. Если получается 4% после уплаты всех налогов — очень хорошо.

Не присматривались к каким-то консервативным вещам вроде облигаций?
Нет, в облигации в нашей стране я не особо хочу вкладывать, а зарубежные облигации не так много дают. Поэтому мне кажется, что инвестиции в недвижимость в нашей стране на данный момент — это консервативный и правильный подход.

У вас же еще была небольшая доля в гольф-клубе «Целеево».
Ну да, я до сих пор миноритарный акционер. Это чисто символическая доля. Я неплохо знаю Олега Дерипаску, мы с ним давние и, можно сказать, хорошие приятели. Он строил этот клуб в какой-то степени под моим влиянием, потому что я очень люблю гольф. Это хобби, которого уже не отнять до конца жизни.
Я даже пытался стать профессионалом, но в один момент понял, что добиться серьезных результатов не получится.

Какие финансовые советы более опытных людей оказались для вас ценными?
Может, мне их и давали, но я не прислушивался. Если бы я мог вернуть время обратно, естественно, постарался бы избежать тех ошибок, которые совершил. Но что для меня важно — я всегда принимал самостоятельные решения. Не хотел создавать ситуацию, когда по чьему-либо совету я бы совершил ошибку и потом винил человека за свой проступок. Уж лучше отвечать буду я, и какое бы решение ни было — хорошее или плохое, — я буду честен перед самим собой. Например, промахи на бирже — моих рук дело, и я никогда не винил в провале своего брокера.

Как бы вы распорядились деньгами, если бы у вас была возможность вернуться на 20-25 лет назад?
Больше бы рисковал, когда был молод. Я бы нырял в стартапы, покупал дешевые акции. В то время $50 тысяч для меня никакой погоды не делали. Потерял — ничего страшного, вложил бы еще столько же и в какой-то момент сорвал бы куш. Сейчас для меня это уже существенные деньги.

Какая доходность для вас комфортна?
Наверно, 8-10% годовых. Я поддерживаю свою семью, родителей и т. д. Естественно, расходов много. Мне 45 лет, и я уже перешел в ту стадию, когда самолеты и яхты не нужны.

Как заработать миллион и остаться при этом человеком?
Это все от воспитания зависит. Некоторых людей деньги сильно портят. Но в то же время они дают независимость — это самое главное. Я в этом плане очень благодарен судьбе, что чувствую себя независимым.

А что бы вы посоветовали в плане финансов нашим читателям?
Я считаю, что усердный труд открывает возможности. Конечно, не обойтись и без счастливого случая, ведь у многих очень умных, талантливых людей не было возможности себя проявить в силу объективных причин. В то же время некоторые успешные люди оказались в нужное время в нужном месте.
Но в целом я уверен, что каждому человеку в жизни предоставляется хотя бы один шанс все кардинально поменять в лучшую сторону. Нужно просто осознать: вот он — и правильно им воспользоваться.

Евгений Кафельников, российский теннисист, заслуженный мастер спорта России

Наиболее важные корпоративные события и отраслевые мероприятия из жизни ИК «Фридом Финанс»

Международное рейтинговое агентство S&P присвоило рейтинг Freedom Finance

Агентство S&P Global Ratings 1 июля присвоило рейтинги на уровне «B-/B» группе компаний Freedom Finance. Также АО «Фридом Финанс» получило рейтинг по национальной шкале на уровне «kzBB-». Прогноз «стабильный» по бизнесу компании отражает ожидания по увеличению объемов комиссионных доходов, отметили аналитики агентства. Согласно рэнкингу S&P, в категории «B-/B» находятся компании, которые имеют возможность в полной мере исполнять свои финансовые обязательства перед клиентами и контрагентами.

Индекс «Фридом — лидеры технологий» запущен на Санкт-Петербургской бирже

Санкт-Петербургская биржа с 17 июля 2019 года начала рассчитывать первый фондовый индекс «Фридом — Лидеры технологий», созданный в партнерстве с ИК «Фридом Финанс». В базу его расчета вошли 10 ведущих американских компаний с капитализацией более $50 млрд и торгующиеся на Санкт-Петербургской бирже: Microsoft Corporation, Amazon.com, Apple, Facebook, Alphabet, Cisco Systems, Netflix, PayPal, Salesforce.com и NVIDIA. Индекс выступает индикатором для биржевого паевого инвестиционного фонда «Фридом — лидеры технологий», который вскоре будет запущен на Московской бирже.

ИК «Фридом Финанс» выступила организатором IPO компании ММЦБ на Московской бирже

25 июля состоялось первичное размещение акций ПАО «Международный Медицинский Центр Обработки и Криохранения Биоматериалов» на Московской бирже. Организатором IPO выступила ИК «Фридом Финанс». Технический андеррайтер размещения — ООО «АЛОР+».

Инвесторам стали доступны более 223 тысяч обыкновенных именных акций, стоимость одной бумаги при размещении составила 672 рубля. Заявки на весь объем размещения были собраны в течение первого часа. В результате IPO компания привлекла более 150 млн рублей, ее рыночная стоимость составила 1 млрд рублей.

ФФИН Банк — лауреат премии им. П. А. Столыпина

В Москве 30 мая состоялось вручение Ежегодной международной премии в области экономики и финансов имени П. А. Столыпина. Высокая награда каждый год вручается за выдающиеся результаты в финансовой и экономической сферах. В этом году в категории «инвестиционные банки» победу одержал ФФИН Банк. Жюри премии высоко оценило его работу по внедрению инновационных продуктов и присудило награду как «Лучшему инвестиционному банку».

Astana Finance Days 2019

Глава Freedom Holding Тимур Турлов выступил спикером панельной сессии на III Международном форуме рынков капитала в городе Нур-Султан. Тема сессии: «Перспективы развития рынка капитала на развивающихся рынках». Участники обсудили доступность технологической инфраструктуры, экосистему брокеров и инвесторов, а также инвестиционные продукты. Глава холдинга поделился своим видением развития отрасли и вариантами преодоления препятствий развивающегося рынка.

Бесплатный семинар для частных инвесторов «Как торговать на фондовом рынке»

В конце мая компания «Фридом Финанс» приняла участие в семинаре, организованном Казахстанской фондовой биржей для розничных инвесторов. Его целью является повышение уровня осведомленности населения Казахстана об отечественном фондовом рынке и его возможностях. Слушатели получили дополнительные знания об инфраструктуре фондового рынка и его основных элементах и инструментах.

FREEDOM finance | Life

7775

www.ffin.life

FREEDOM finance

Лицензия на осуществление деятельности на рынке ценных бумаг 3.2.238/15 от 02 октября 2018 года. www.almaty-ffin.kz. Реклама.

7555