

# АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ — 2017

---

## ТРЕНДЫ И ПРОГНОЗЫ

## СОДЕРЖАНИЕ

Тренды-2017 .....	3
Итоги года .....	4
Использование вредоносного ПО .....	7
Социальная инженерия .....	7
Компрометация учетных данных .....	8
Эксплуатация веб-уязвимостей .....	9
Использование уязвимостей ПО .....	9
DDoS .....	10
Атаки по отраслям .....	11
Государственные организации .....	11
Финансовая отрасль .....	12
Онлайн-сервисы .....	13
Медицинские учреждения .....	14
Образование .....	15
Сфера услуг .....	16
IT-компании .....	17
Промышленные компании .....	18
Розничная торговля .....	19
Частные лица .....	20
Прогнозы .....	21

## ТРЕНДЫ-2017

На протяжении года мы ежеквартально делились информацией об актуальных угрозах информационной безопасности, выделяли современные техники и механизмы реализации атак и рассказывали, как правильно организовать защиту от киберпреступников. Этой публикацией мы подведем итоги 2017 года и рассмотрим, как менялось поведение злоумышленников, как отличались методы действий преступников в зависимости от отрасли и чего ожидать от 2018 года.

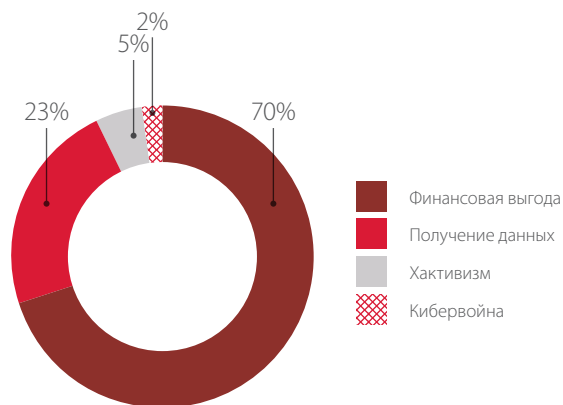
Если кратко, то:

- + Главный тренд 2017 года — трояны-шифровальщики. Причем речь не только о вымогателях, но и тех, что безвозвратно шифруют данные, нанося тем самым огромный урон инфраструктуре компаний.
- + За счет активного продвижения услуги ransomware as a service одни и те же трояны стали многократно использоваться разными лицами, а порог входа в киберпреступный бизнес снизился, ведь через интернет купить вредоносное ПО теперь может любой желающий, не обладающий специальными навыками.
- + Вместе с ростом числа вредоносных кампаний увеличивается и количество пострадавших от них обычных пользователей. Эта тенденция также связана с популярностью ransomware as a service, поскольку новички в киберпреступной среде, которые ищут быстрой наживы, направляют купленные трояны именно на частных лиц.
- + Развивается направление вредоносного ПО, нацеленного на промышленность. Отличительной чертой этих программ является то, что они учитывают специфику инфраструктуры промышленных компаний, и, соответственно, выявить их оказывается намного сложнее.
- + Отдельно стоит отметить вредоносное ПО для POS-терминалов и банкоматов. Несмотря на существенные сложности доставки этого ВПО до конечной цели, именно оно использовалось в каждой восьмой атаке на банк.
- + Самыми похищаемыми данными стали медицинская информация и данные платежных карт. Персональные данные тоже по-прежнему интересуют злоумышленников, однако в даркнете они уже не ценятся так высоко, как раньше.
- + В 2017 году отмечались ажиотаж вокруг криптовалюты и существенный рост популярности ICO (initial coin offering, первичного размещения токенов), который привлек и злоумышленников, направивших атаки на криптовалютные биржи, кошельки частных лиц и ICO-стартапы.
- + В среднем атаки стали содержать больше этапов, а в их выполнении стало участвовать больше людей. Это подтверждается и популярностью таких методов, как supply chain attack и атаки drive-by.
- + Ботнеты продолжили расти за счет новых IoT-устройств, и, как следствие, увеличилась мощность DDoS-атак. Злоумышленники продолжили изобретать новые и модифицировать старые трояны для эксплуатации многочисленных уязвимостей в «умных вещах».
- + Со многими громкими политическими событиями были связаны действия киберпреступников. Кибератака становится действенным методом влияния на общественное мнение и политическим инструментом.
- + В России отношение к вопросам информационной безопасности становится более ответственным как со стороны государства, так и отдельных отраслей. В 2017 году была утверждена программа «Цифровая экономика», одним из векторов которой является обеспечение информационной безопасности. В различных отраслях развиваются центры по противодействию киберугрозам (например, ФинЦЕРТ, КЦПКА), а также создаются центры ГосСОПКА. Это позволяет снизить нагрузку на регуляторов и учесть специфику защиты информационных систем в каждой из отдельных отраслей.

## ИТОГИ ГОДА

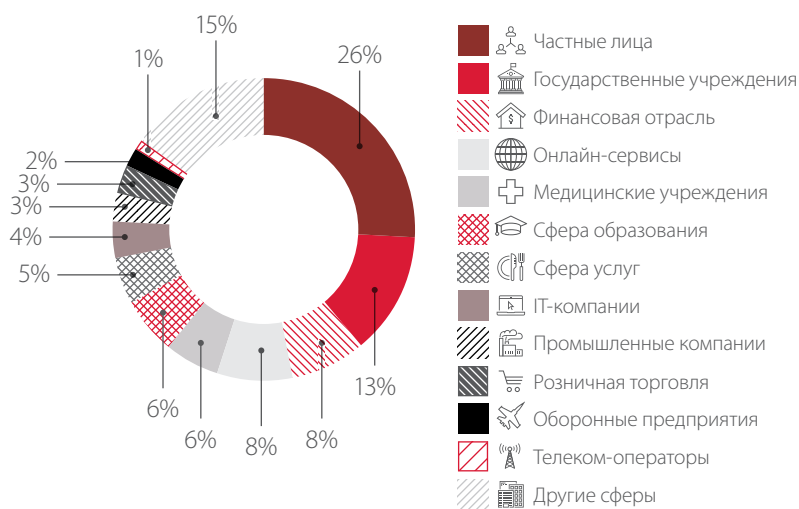
Семь из каждых 10 атак были совершены с целью получения прямой финансовой выгоды (например, за счет вывода денег с банковских счетов жертвы) и еще 23% — с целью получения данных.

Если в первом полугодии доли массовых и целевых атак были примерно равны, то по итогам года большинство составили массовые кибератаки (57%).



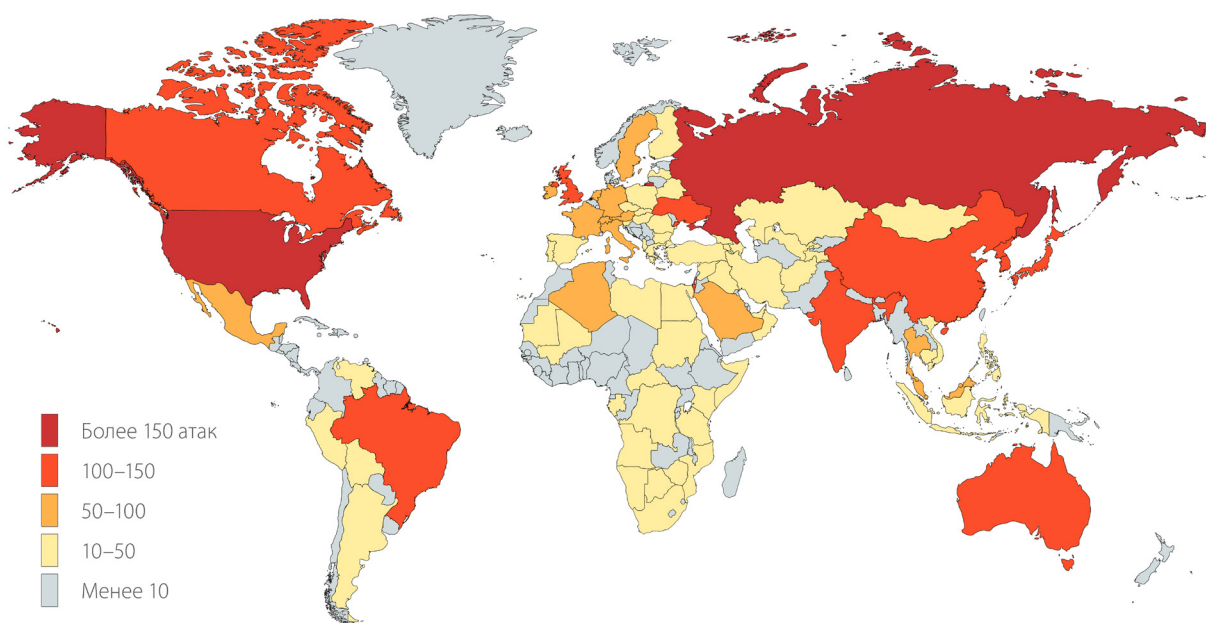
Мотивы злоумышленников

Наибольший интерес злоумышленников был направлен на частных лиц: на них пришлось четверть всех атак (26%). Больше других от кибератак страдали государственные организации (13% атак), банки и онлайн-сервисы (по 8%). В случае масштабных атак, поражающих сотни и тысячи компаний, бывает невозможно отнести инцидент к одной из перечисленных отраслей; в таком случае его относили к категории «Другие сферы», этим объясняется столь существенная ее доля (15%).



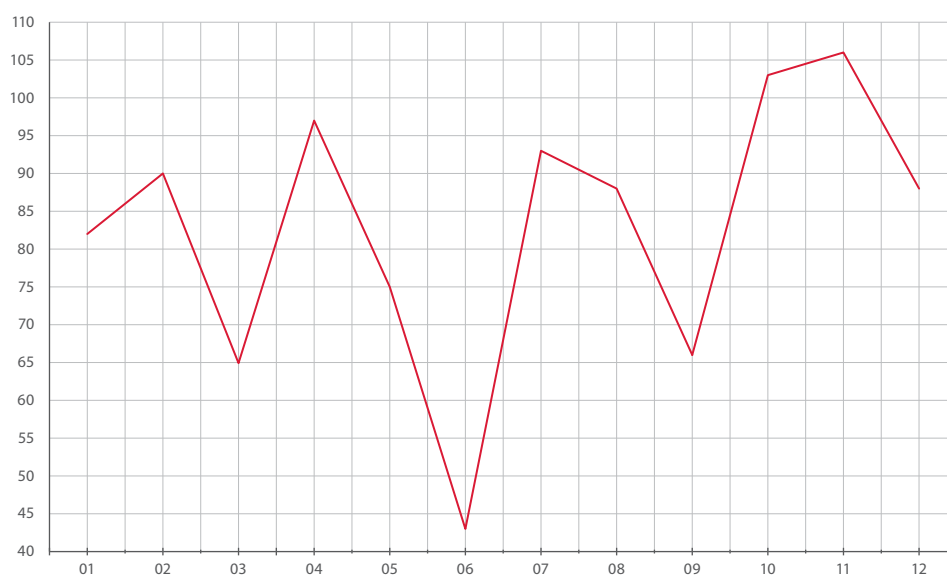
Категории жертв, пострадавших от атак в 2017 году

Для киберпреступников не существует границ между странами и континентами, поэтому все больше атак затрагивают одновременно две, три, десять и более стран. Тем не менее США и Россия в течение 2017 года были абсолютными лидерами по числу киберинцидентов. Это может быть связано с тем, что на эти страны в первую очередь было направлено внимание общественности и СМИ, хотя в целом атакам подвергались не менее 64 стран по всему миру. Наиболее частыми жертвами кибератак становились Великобритания, Австралия, Канада, Индия, Япония, Украина, Израиль и Китай.



География кибератак 2017 года

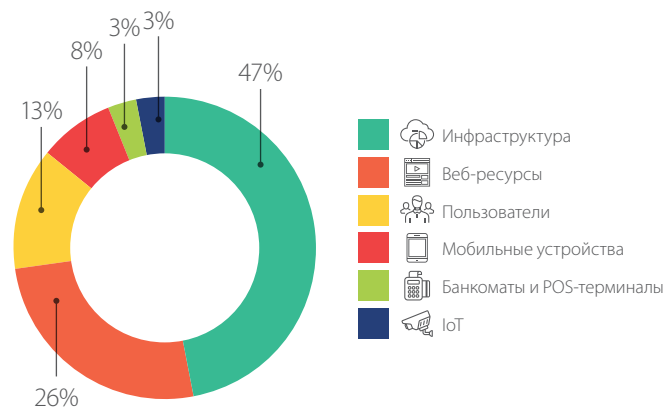
По сравнению с 2016 годом в 2017-м мы зафиксировали на 13% больше уникальных инцидентов. Наибольшее количество кибератак снова пришлось на IV квартал, а наименьшее — на второй. В течение последних двух лет мы наблюдаем такие закономерности, как спад хакерской активности в мае-июне и ее увеличение под конец года.



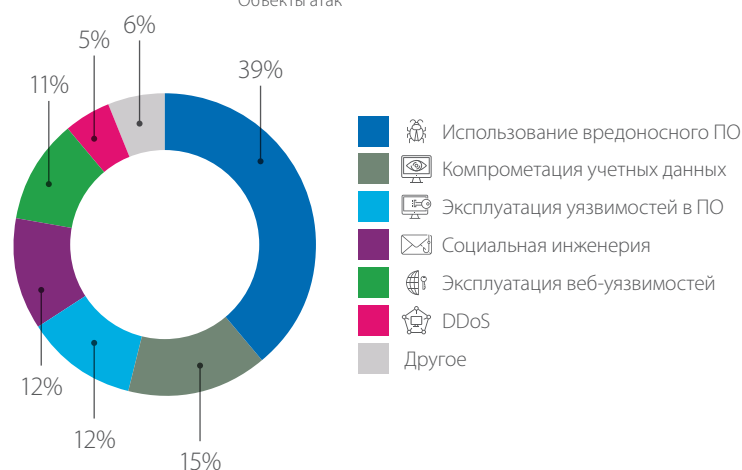
Количество кибератак в 2017 году

По итогам 2017 года самыми частыми объектами атак стали инфраструктура и веб-ресурсы компаний, доли таких атак составили 47% и 26% соответственно. Стоит также отметить, что мы наблюдали увеличение числа атак на банкоматы и POS-терминалы: оно превысило показатели 2016 года в 7 раз и, вероятно, продолжит расти в 2018 году.

При анализе инцидентов мы рассматривали только уникальные события, поэтому все происшествия, связанные с заражением одним трояном или его модификациями, учитывались как один масштабный инцидент. Наибольшее число атак было совершено с использованием вредоносного ПО, их доля составила 39%. Более подробную статистику по использованию различных методов при реализации кибератак мы рассмотрим далее.



Объекты атак



Методы атак

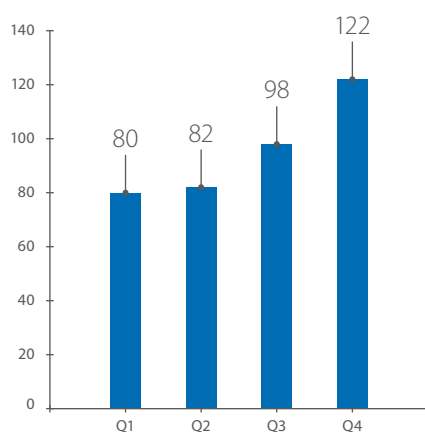
		Отрасль											
		Финансовая отрасль	Государственные учреждения	Медицинские учреждения	Сфера образования	Промышленные компании	Онлайн-сервисы	Сфера услуг	Частные лица	Розничная торговля	IT-компании	Телеком-операторы	Другие сферы
Объект	Инфраструктура	32	73	34	33	23	15	22	89	6	20	3	112
	Веб-ресурсы	25	45	6	10	1	54	16	47	14	12	2	23
	Пользователи	8	8	21	15	5	5	4	46	1	2	1	13
	Банкоматы и POS-терминалы	12						7	1	6	1		2
	Мобильные устройства		3					3	70		1	1	3
	IoT		5				1	1	5		2	2	13
Метод	Атаки с использованием ВПО	40	39	16	16	12	4	17	136	8	15	1	78
	Компрометация учетных данных	2	20	13	14	4	16	14	35	4	4	1	21
	DDoS	7	19	1			10	2		2	4	1	4
	Социальная инженерия	12	9	12	9	8	2	2	38	2	2	1	21
	Эксплуатация уязвимостей в ПО	8	20	8	9	2	13	3	20	3	5	2	26
	Эксплуатация веб-уязвимостей	9	19	7	8	1	27	9	12	5	3	1	7
	Другой	2	8	4	2	2	3	6	14	3	5	2	9
Мотив	Финансовая выгода	74	59	42	47	16	64	37	202	20	32	7	93
	Получение данных	6	45	17	10	7	7	11	49	7	6	2	59
	Хактивизм		23	2	1	2	4	5	2				9
	Кибервойна		7			4			2				5

Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) и отраслям

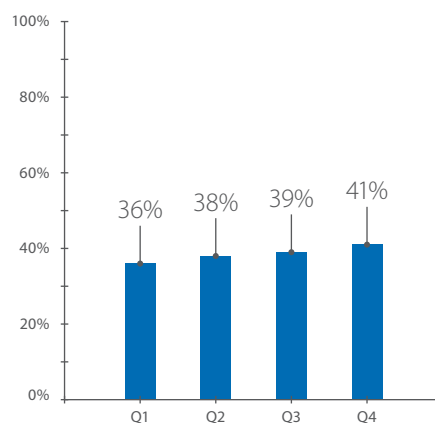


Ущерб от атак с использованием вредоносного ПО в 2017 году составил **более 1,5 млрд долл. США**

## ИСПОЛЬЗОВАНИЕ ВРЕДНОСНОГО ПО



Количество атак с использованием ВПО



Доля атак с использованием ВПО

В первой половине 2017 года особой популярностью у злоумышленников пользовались трояны-вымогатели. Помимо нашедших эпидемий Wannacry и NotPetya было множество других вредоносных кампаний, нацеленных на вымогательство денег у жертв (например, Jaff или SOREBREX).

В течение года мы наблюдали рост популярности модели «вымогатели как услуга» (ransomware as a service), при которой авторы вредоносного ПО не являются организаторами атак, а зарабатывают на продаже троянов преступным группировкам — чаще всего для проведения массовых атак. Таким образом разработчики вредоносного ПО, получив прибыль от продажи, могут готовить новый троян в то время, как другие преступники занимаются непосредственно реализацией атаки. Это привело к тому, что существенно снизился порог входа в киберпреступный бизнес, ведь приобрести вредоносное ПО теперь может любой желающий.

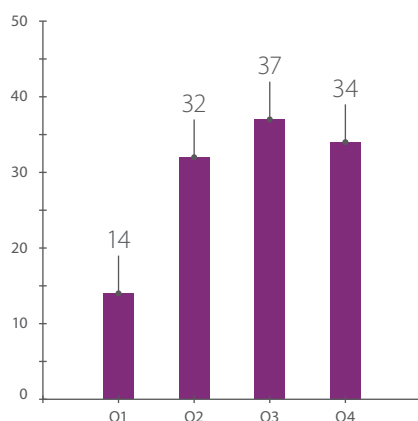
В конце года мы отметили тенденцию к использованию вредоносного ПО для сокрытия истинных мотивов киберпреступных действий, а также для уничтожения следов преступления. Причем данные в ходе таких атак часто уничтожались безвозвратно, и при проведении расследования становилось невозможно восстановить все детали и последовательность событий.

Во второй половине года вместе с ростом курса биткойна выросла и популярность майнеров криптовалюты. Пользователей охватила волна атак, пожирающая вычислительные мощности устройств. Злоумышленники использовали вредоносное ПО для генерации криптовалюты на компьютерах, серверах и мобильных телефонах жертв.

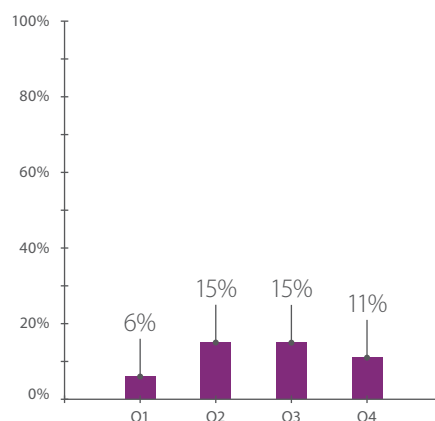
## СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



Ущерб от атак методом социальной инженерии в 2017 году составил **более 250 млн долл. США**



Количество атак методом социальной инженерии



Доля атак методом социальной инженерии

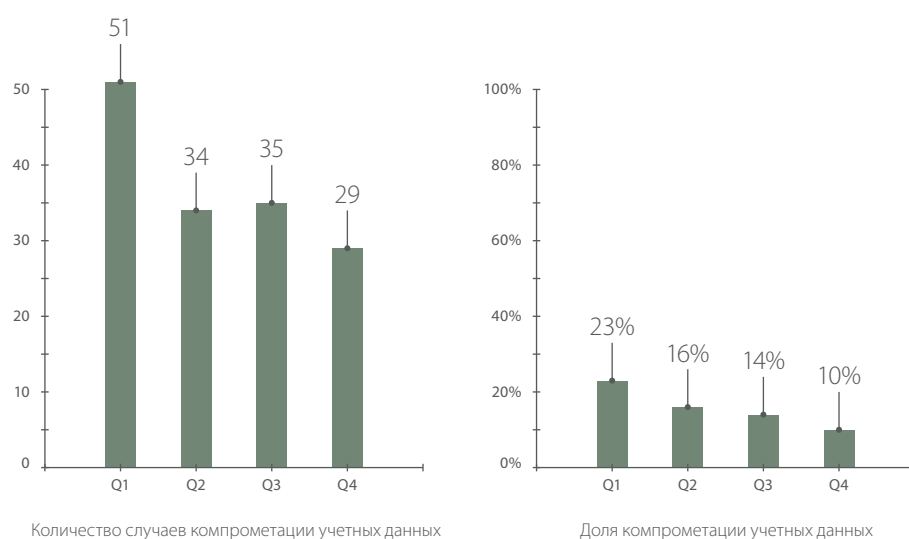
В 2017 году злоумышленники продолжили совершенствовать методы социальной инженерии. Наиболее часто они использовали фишинговые сайты и фишинговые рассылки для целевых атак на организации. Чтобы письма выглядели правдоподобно, они подделывали адреса отправителей, регистрировали домены, похожие на доверенные, и даже взламывали контрагентов, чтобы отправлять письма от их имен в обход спам-фильтров.

Большое количество кибератак было направлено и на обычных пользователей. В ходе таких атак злоумышленникам, как правило, требовались банковская информация (номера карт, учетные данные онлайн-банкинга), а также учетные данные различных онлайн-сервисов и электронной почты. Для их получения преступники подделывали веб-сайты, с помощью писем доставляли на компьютер жертв вредоносное ПО, в СМС-сообщениях убеждали перейти по ссылке на фишинговый ресурс или просто уговаривали сообщить по телефону всю необходимую информацию.

## КОМПРОМЕТАЦИЯ УЧЕТНЫХ ДАННЫХ



Ущерб от компрометации учетных данных в 2017 году составил **более 100 млн долл. США**



Итоги 2017 года показали, что если в компании плохо настроена парольная политика, то злоумышленники могут легко подобрать пароль, а потом использовать полученные учетные данные для того, чтобы попасть в корпоративную информационную систему. Кроме того, зачастую пароли хранятся в базах данных в незашифрованном виде, и в случае утечки такой базы злоумышленникам даже не приходится тратить время на подбор паролей по хеш-функциям.

Мир помешался на криптовалюте, и пока одни регистрировали криптокошельки и переводили на них деньги, другие подбирали учетные данные к этим кошелькам и забирали себе хранящиеся там средства.

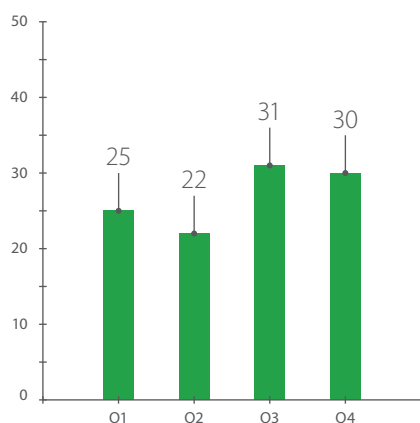
Компрометация учетных данных от IoT-устройств привела к тому, что миллионы роутеров, IP-камер, пылесосов и прочей утвари оказались в ботнетах и используются для майнинга криптовалюты, слежки за людьми и DDoS-атак.



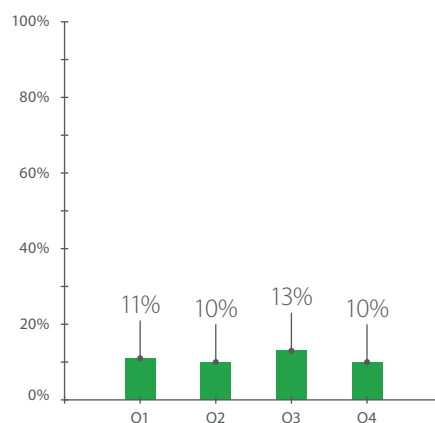


Ущерб от атак с использованием веб-уязвимостей в 2017 году составил **более 390 млн долл. США**

## ЭКСПЛУАТАЦИЯ ВЕБ-УЯЗВИМОСТЕЙ



Количество атак с использованием веб-уязвимостей



Доля атак с использованием веб-уязвимостей

Атаки на площадки ICO стали одним из главных трендов 2017 года, а недостаточная защищенность веб-ресурсов, предназначенных для проведения ICO, обошлась организаторам в миллионы долларов. Например, в результате атаки на [CoinDash](#) злоумышленники присвоили себе 9 млн долларов инвестиций.

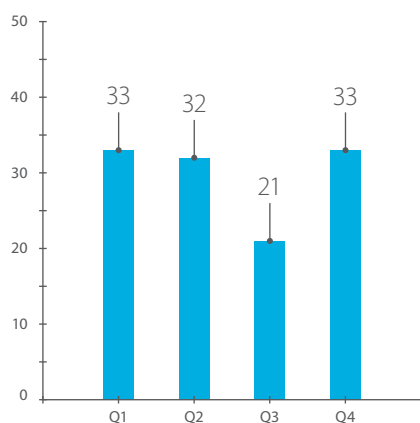
Веб-сайты государственных структур стали излюбленной мишенью хактивистов. Государственные учреждения, в частности министерства, представляют собой лицо государства, в первую очередь в глазах СМИ, в том числе зарубежных. Именно поэтому различные хактивисты выбирают их своими целями для дефейса, а затем публикуют на них различные агитационные материалы.

Злоумышленники стали использовать уязвимые сайты в качестве хостинга для вредоносного ПО и атак drive-by. А для того, чтобы как можно больше человек зашли на веб-ресурс, киберпреступники используют SEO-методы для поднятия сайта в поисковой выдаче. Для этого они размещают на скрытых страницах специально отобранные ключевые слова, а рейтинг увеличивают с использованием SEO-ботнетов. Используемые в качестве хостинга сайты по сути становятся промежуточным звеном в цепочке атаки, а их владельцы — невольными соучастниками преступлений. Это может нанести серьезный ущерб их репутации, а также привести к блокировке веб-ресурсов регулятором или изъятию серверного оборудования правоохранительными органами при проведении расследования. Таким образом, даже не являясь мишенью злоумышленников, любой сайт может оказаться атакованным.

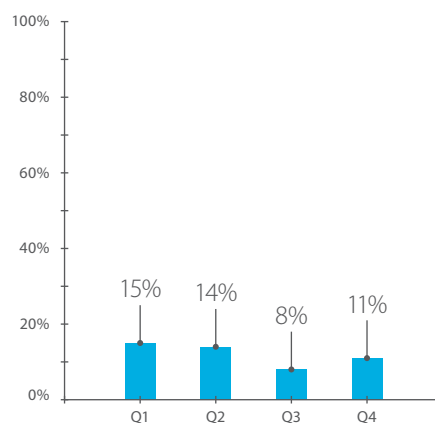
## ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ ПО



Ущерб от атак с использованием уязвимостей ПО в 2017 году составил более **280 млн долл. США**



Количество атак с использованием уязвимостей ПО



Доля атак с использованием уязвимостей ПО

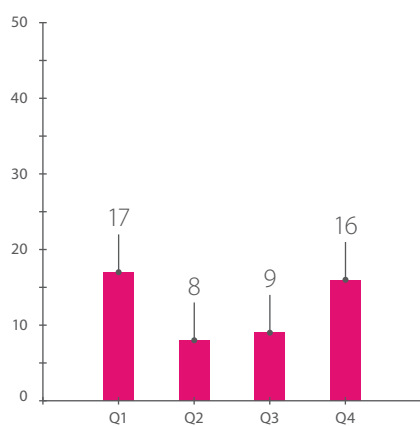
В ходе тестов на проникновение наши специалисты регулярно выявляют использование устаревших версий программного обеспечения или отсутствие необходимых обновлений безопасности. А значит, нарушитель может использовать известные уязвимости, характерные для этих версий ПО, в реализации различных атак. В даркнете даже можно найти и купить готовые эксплойты, которые позволят быстро воспользоваться уязвимостью и, например, получить доступ к базе данных на сервере.

Кроме того, в ходе сложных целенаправленных атак злоумышленники часто используют уязвимости нулевого дня для того, чтобы их действия в корпоративной информационной системе как можно дольше оставались незамеченными. Например, уязвимость нулевого дня в Apache Struts, [CVE-2017-5638](#), принесла киберпреступникам порядка 100 тысяч долларов. С помощью этой уязвимости, позволяющей выполнять произвольные команды на веб-сервере, злоумышленники устанавливали на серверах бэкдоры, ботов для DDoS-атак, ПО для майнинга криптовалюты и программы-вымогатели.

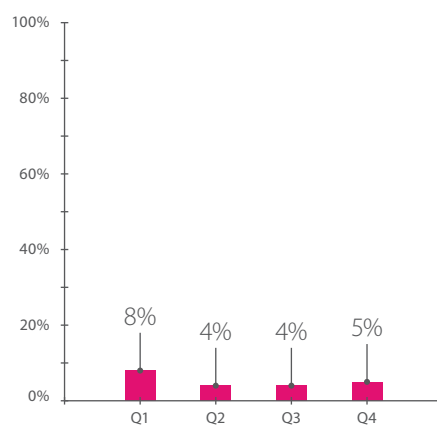
## DDOS



Сумма ущерба  
от DDoS-атак  
не установлена



Количество атак с использованием уязвимостей ПО



Доля атак с использованием уязвимостей ПО

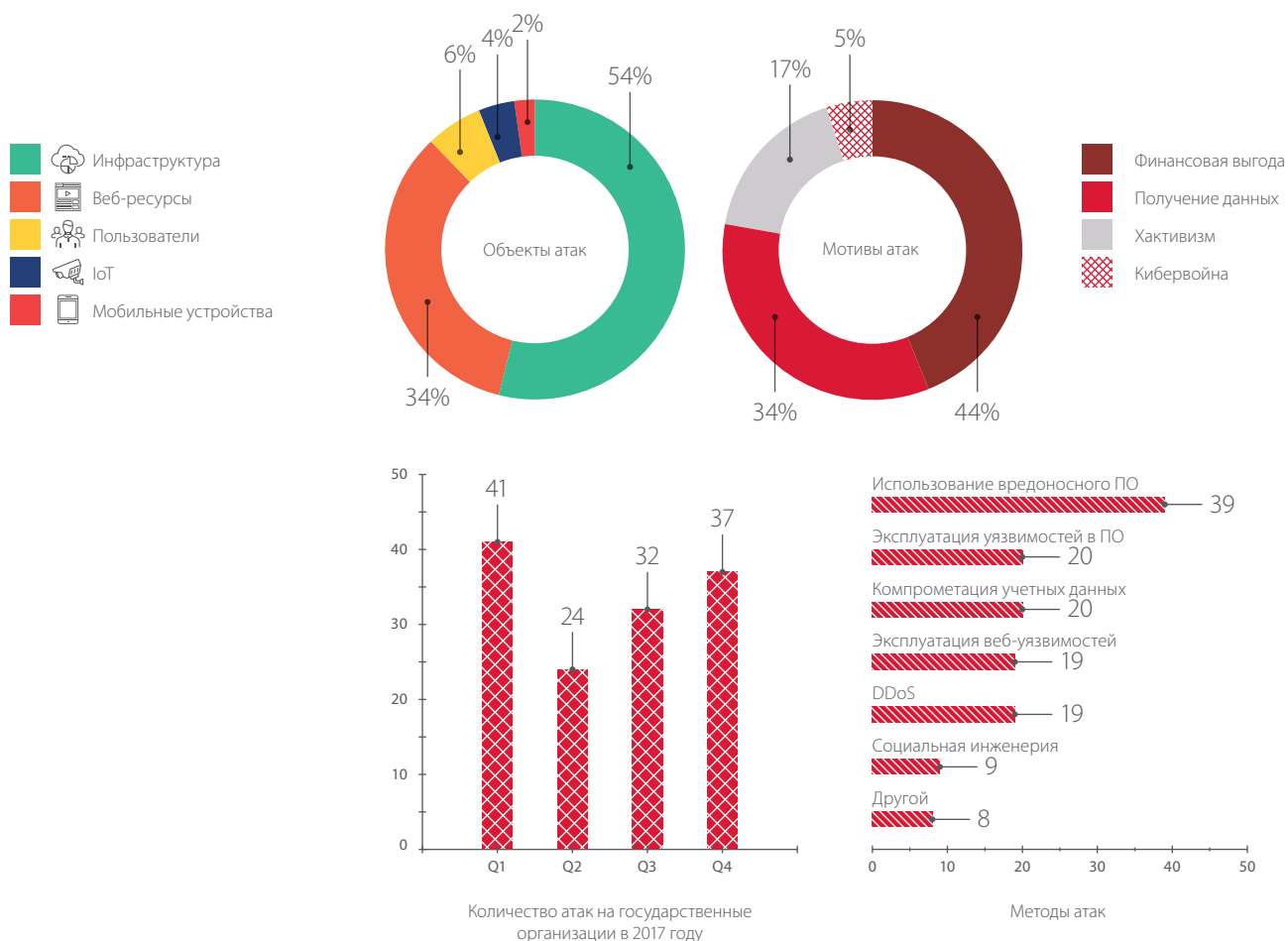
Временное отсутствие доступа к веб-ресурсу на первый взгляд может показаться мелочью. Но на самом деле в результате DDoS-атак компании теряют не только крупные суммы денег, но и лояльность клиентов. Действительно, невозможность совершить перевод или платеж через онлайн-банк в течение нескольких часов вызовет недовольство среди клиентов, которые усомнятся в надежности банка, а возможно — понесут финансовые потери из-за сорванной сделки.

От DDoS-атак в 2017 году преимущественно страдали государственные компании (как правило, из-за действий хактивистов), онлайн-сервисы (например, криптовалютные биржи или платформы для проведения ICO) и финансовые организации. Еще раз подчеркнем, что учитывались только уникальные DDoS-кампании, и в случае если жертвами атак одного ботнета становилось множество организаций, эта массовая атака считалась как один инцидент.

## АТАКИ ПО ОТРАСЛЯМ

Далее мы подробнее остановимся на анализе атак на отдельные отрасли, которые в течение 2017 года чаще других становились целью злоумышленников.

### Государственные организации

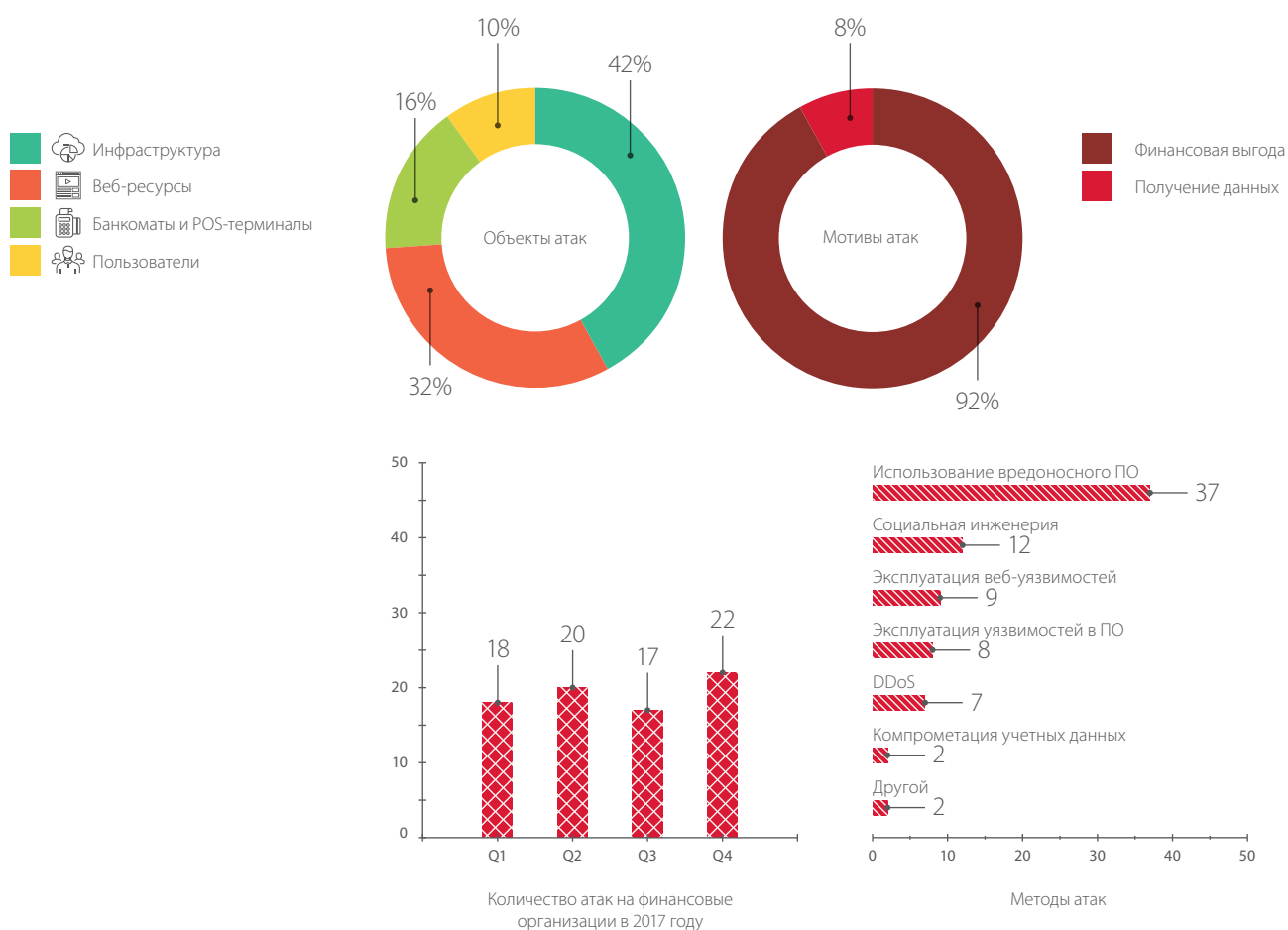


На государственные организации были направлены 13% всех атак. С атаками на госсектор часто связывают хакерские группировки (например, OilRig, Turla, Lazarus). В различных исследованиях можно встретить характеристику действий одной и той же группировки, но под разными названиями. Поэтому точно подсчитать общее количество действующих в настоящее время группировок довольно затруднительно, но по нашим оценкам в 2017 году их было не менее 70.

Примечательно, что несколько атак с использованием вредоносного ПО были нацелены на личные мобильные телефоны госслужащих. Из-за того, что сотрудники часто проверяют в свободное время рабочую почту со смартфонов, злоумышленникам становилась доступна конфиденциальная информация, касающаяся организации, в которой они работали.

Треть атак на государственные организации (34%) была направлена на получение данных (шпионаж). В атаках такого рода главной целью злоумышленников является получение доступа к внутренним ресурсам компании и защищаемой информации. Кроме того, получив доступ к серверам, злоумышленники могут делать все, что им вздумается: могут затаиться и ждать подходящего момента, а могут вывести из строя серверное оборудование или уничтожить базы данных.

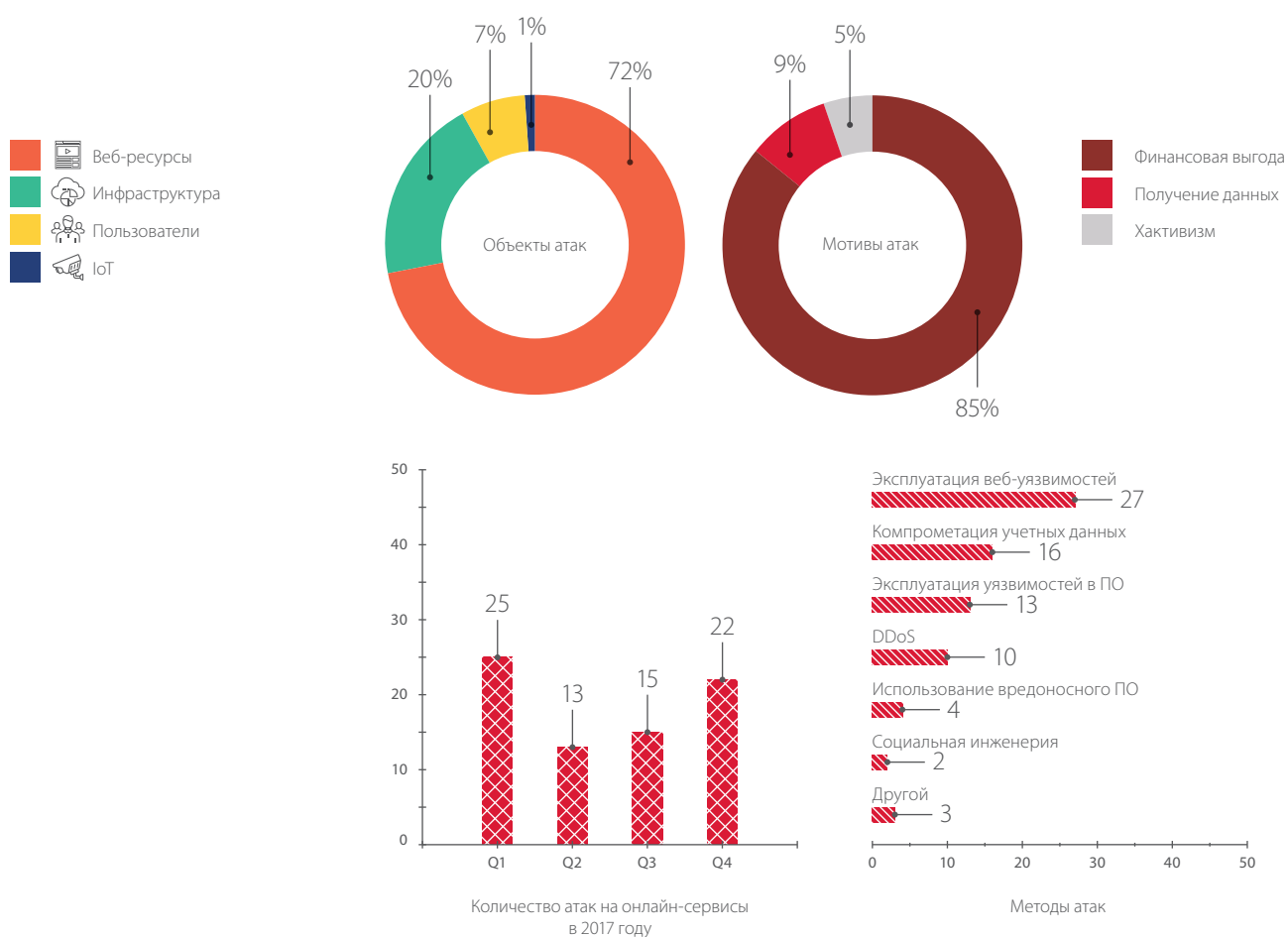
## Финансовая отрасль



Финансовая отрасль не теряет привлекательности для злоумышленников. В половине атак на банки в 2017 году было задействовано вредоносное ПО. Причем существенна доля атакованных POS-терминалов и банкоматов. По сравнению с результатами 2016 года отмечается значительный рост этой категории атак. Именно при помощи вредоносного ПО злоумышленники пытались или получить доступ непосредственно к банкоматам и управлять выдачей денег из них, или скомпрометировать внутренние ресурсы банка.

Нельзя не отметить действия группировки Cobalt, за активностью которой мы следим уже второй год. Целью этих хакеров обычно является попадание в локальную сеть банка. Как правило, для этого они используют фишинговые рассылки сотрудникам банка. Чтобы пройти спам-фильтры компании и увеличить вероятность прочтения письма, они регистрируют домены, похожие на доверенные (например, visa-pay.com, swift-alliance.com, cards-cbr.ru, billing-cbr.ru), или компрометируют инфраструктуру контрагентов (поставщиков оборудования, страховых компаний) и отправляют от их имени письма, содержащие вредоносные вложения. Проникнув в ЛВС банка, злоумышленники исследуют сеть в поисках компьютеров сотрудников, отвечающих за работу банкоматов, загружают через них на АТМ вредоносное ПО и получают доступ к удаленному управлению банкоматами. В установленное время (как правило, ночью) к определенному банкомату подходят «мулы» и забирали деньги.

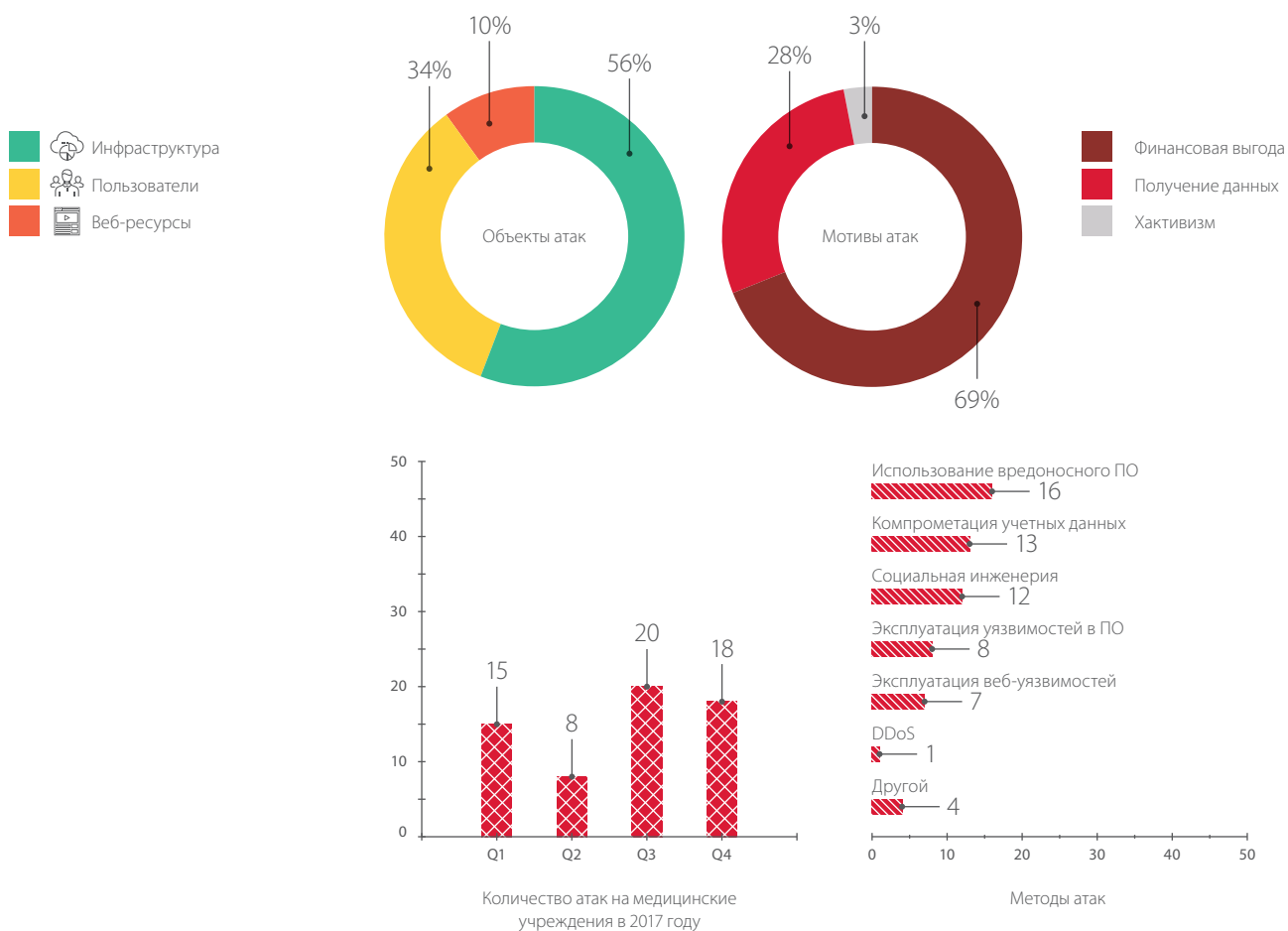
## Онлайн-сервисы



Объем инвестиций, привлеченных с помощью ICO в 2017 году, превысил 5 млрд долл. США. Самые прибыльные проекты принесли своим компаниям 883,4 млн (EOS), 257 млн (Filecoin) и 232 млн (Tezos). Но кроме капитала ICO привлек также и злоумышленников. По различным данным, в 2017 году через ICO было похищено порядка 300 млн долларов, что составило около 7% всех заработанных за этот год на ICO средств.

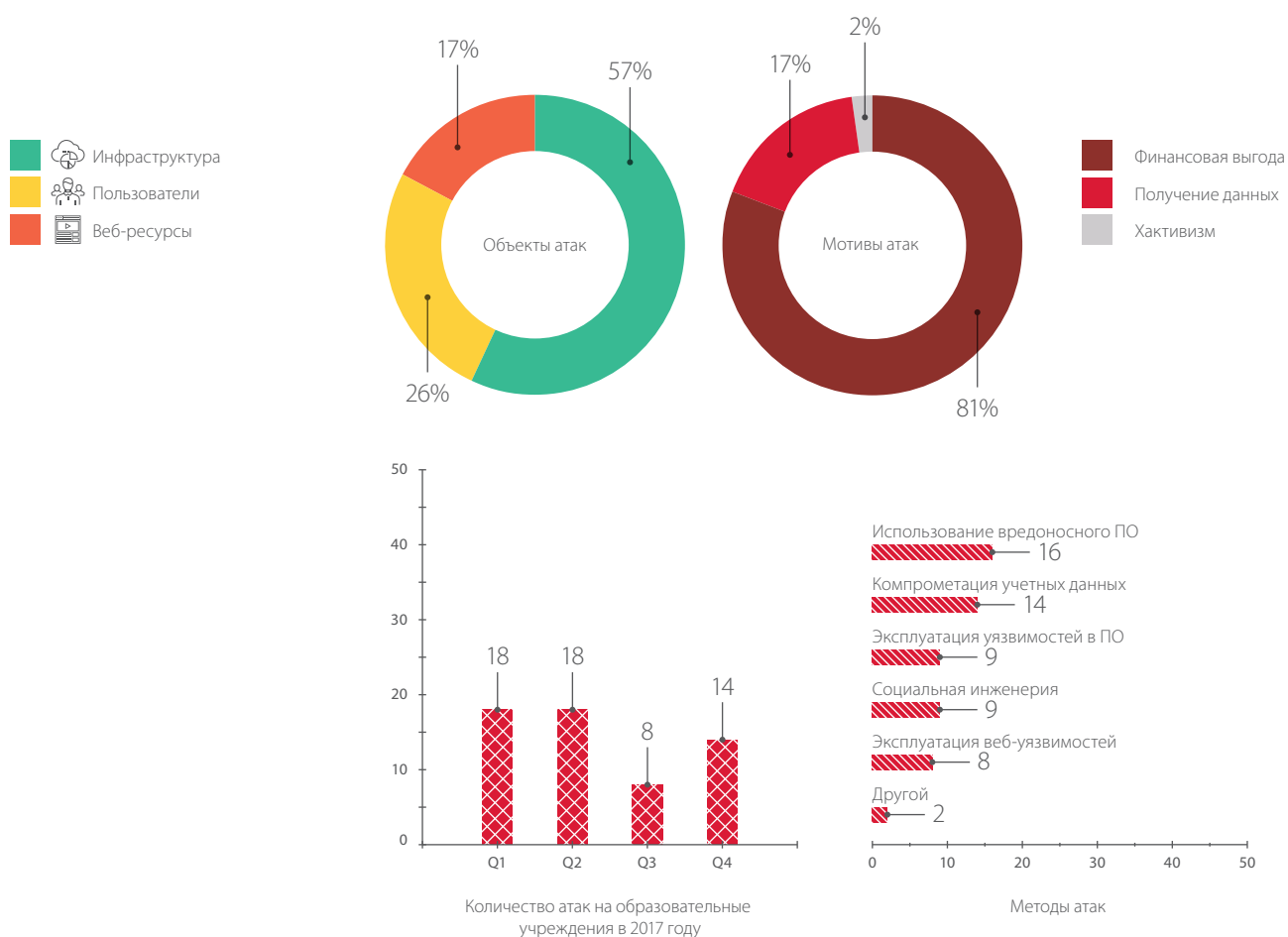
В атаках на ICO злоумышленники чаще всего старались получить контроль над платформой, чтобы подменить адрес кошелька организаторов на свой. Для этого они использовали уязвимости в веб-приложениях, проводили атаки на организаторов (например, получали доступ к электронной почте, а затем восстанавливали пароли от домена или хостинга). Кроме того, в ходе атак на ICO часто применялись фишинг в адрес инвесторов (например, создавались поддельные сайты или отправлялись письма об изменении контактов организаторов и кошелька для сбора средств) и поиск ошибок в коде смарт-контрактов.

## Медицинские учреждения



Медицинские сведения более 2 млн человек в 2017 году стали доступны злоумышленникам в результате атак на медучреждения. Примечательно, что эта информация востребована на черном рынке и оценивается в 10–15 раз выше паспортных данных. В половине атак (56%) киберпреступники проникали во внутреннюю сеть организации (например, в результате фишинговой рассылки в адрес сотрудников или подобрав пароли от учетных записей) и получали доступ к серверам и базам данных.

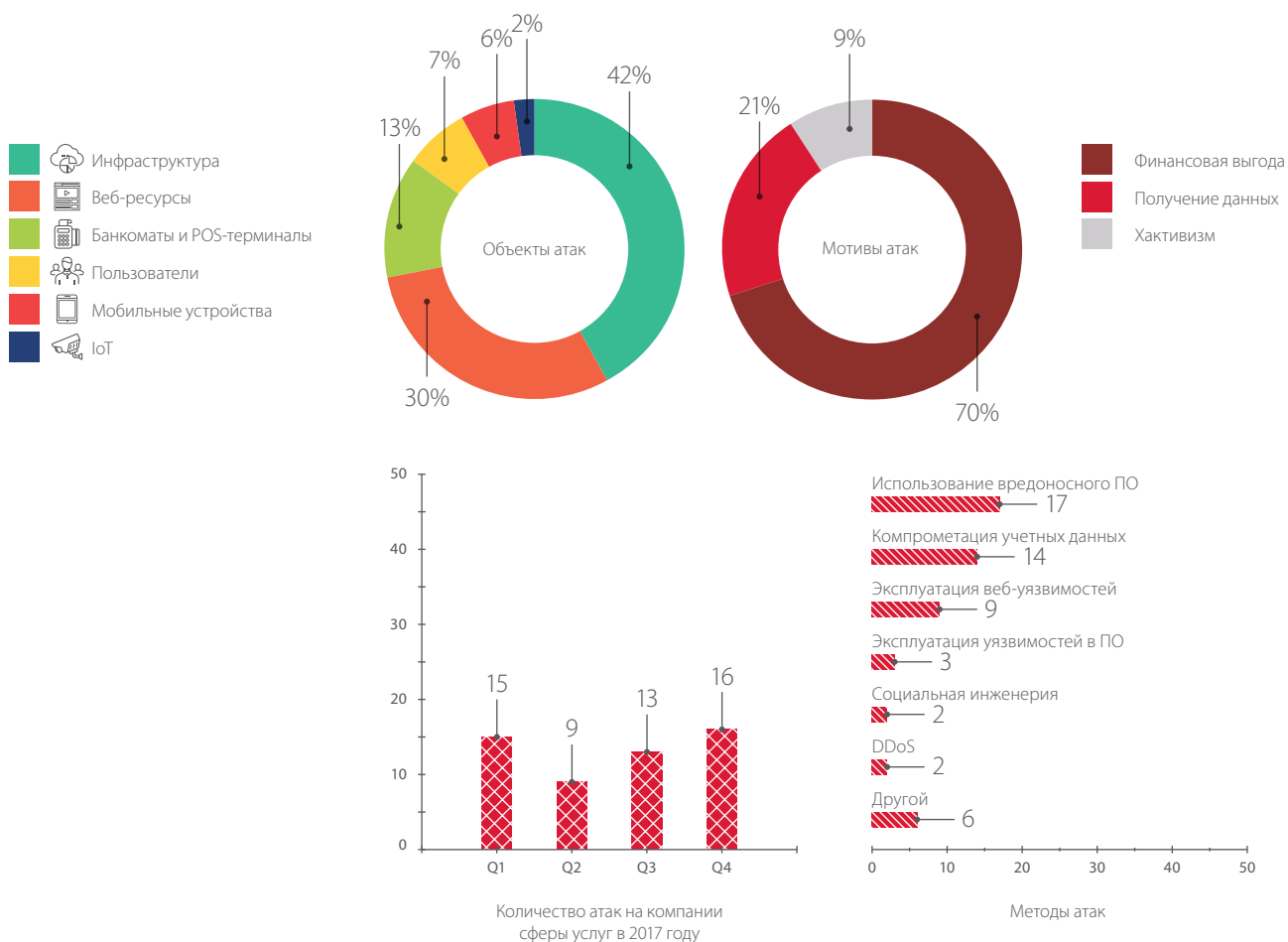
## Образование



Образовательные учреждения часто становятся жертвами самих учащихся. Причем речь идет не только об университетах, где обучают, среди прочего, навыкам программирования, но и об обычных общеобразовательных школах. Ученики находят в интернете вредоносное ПО и с его помощью взламывают компьютерную систему учебного заведения, чтобы подменить оценки на более высокие. Примечательно, что эти школьники обычно не задумываются о последствиях своих противоправных действий и легко оказываются в руках правоохранительных органов.

Однако образовательным учреждениям стоит бояться не только учеников, но и более профессиональных хакеров. Еще один популярный мотив атак на учебные учреждения это получение персональных данных об учащихся, в которых обычно содержится такая информация как адрес проживания, адреса электронной почты родителей, места их работы. Эти данные могут быть использованы в целевой атаке на компанию, в которой работают родители. Финансовую выгоду, как правило, киберпреступники получали, требуя выкуп у самих образовательных учреждений (например, за восстановление данных) или продавая свои услуги по взлому (например, для подмены оценок в системе).

## Сфера услуг

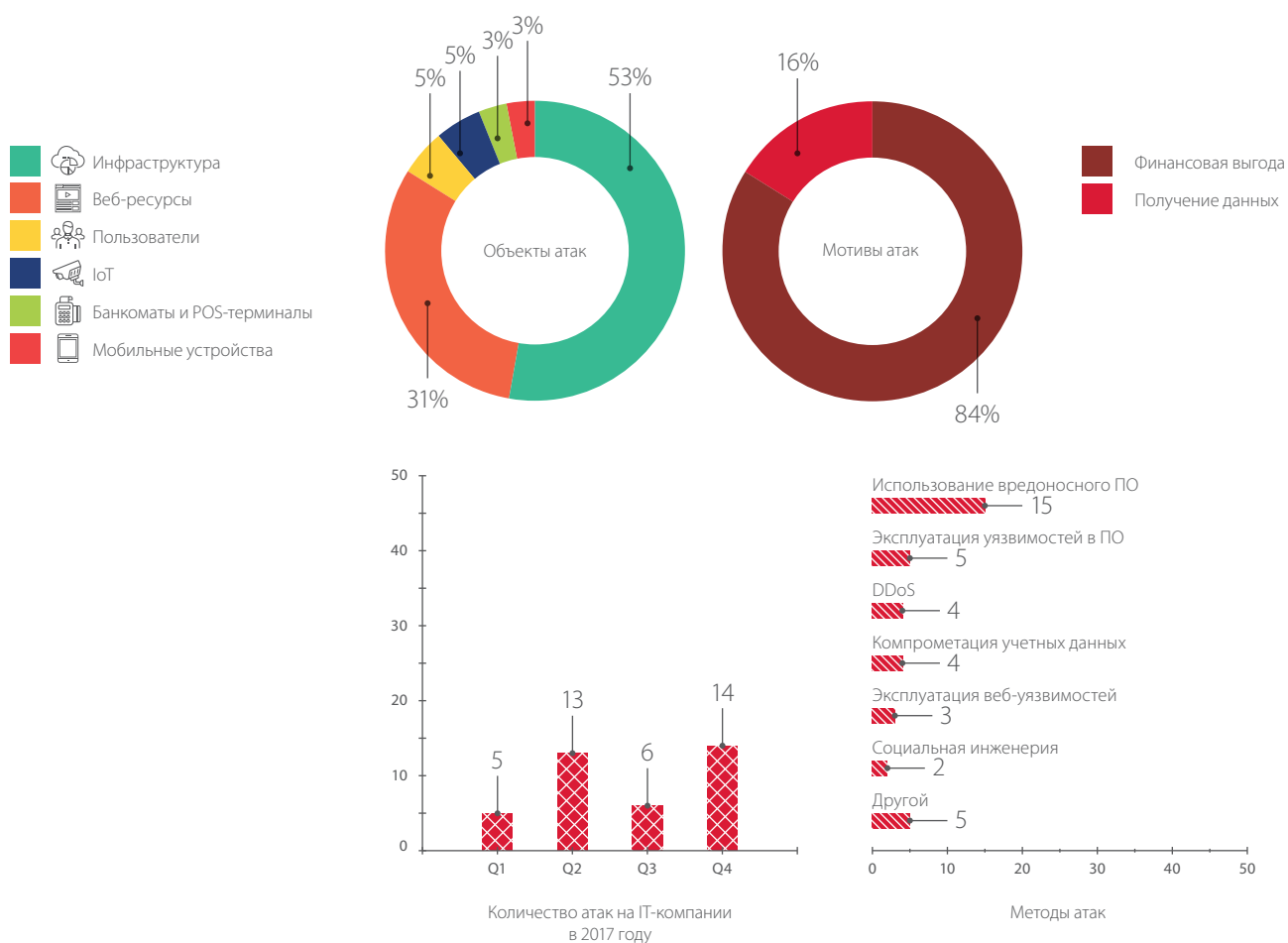


В сфере услуг в 2017 году большое количество инцидентов было связано с кражей данных банковских карт при помощи вредоносного ПО для POS-терминалов. Особенно от них страдали клиенты ресторанов быстрого питания и гостиницы.

Примечательно, что если недостатки в реализации защиты информационных ресурсов компании позволили злоумышленникам атаковать пользователей и, например, похитить их деньги или получить персональные данные, то потери понесет не только клиент, но и сама компания — из-за репутационных рисков.

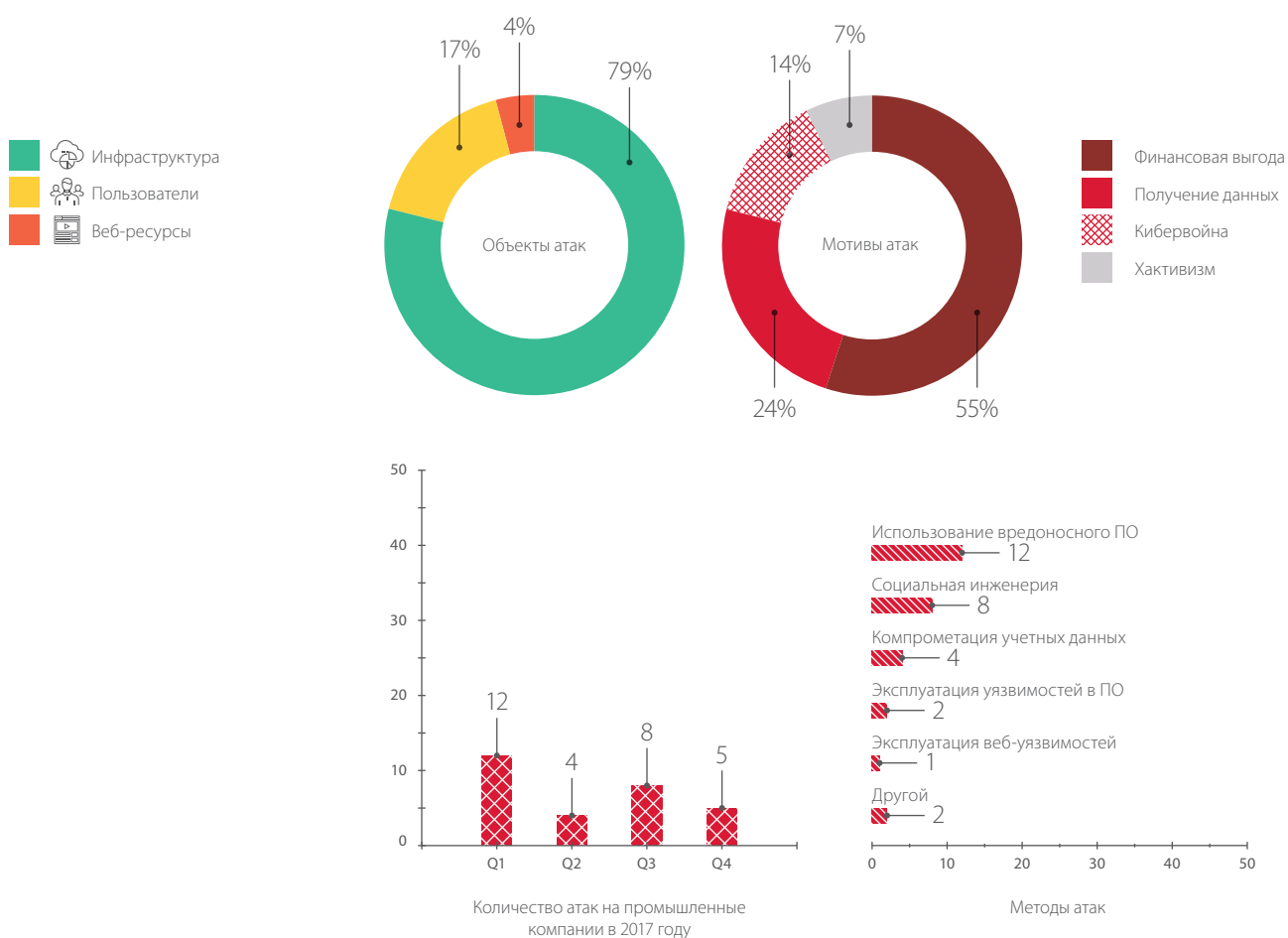


## IT-компании



Атаки на IT-компании не выделялись на фоне других организаций. Однако стоит отметить, что в 2017 году целью злоумышленников не раз оказывались компании, занимающиеся вопросами информационной безопасности. Киберпреступники пользовались доверием людей к сайтам ИБ-компаний и распространяли, например, с их помощью вредоносное ПО. Отметим, что абсолютно любая компания вне зависимости от сферы деятельности может оказаться посредником в цепочке целенаправленных атак. Этот метод называется *supply chain attack* и подразумевает компрометацию одной компании для атаки на другую, например на ее партнера. Особенно часто используется он для отправки фишинговых рассылок, поскольку позволяет обойти спам-фильтры.

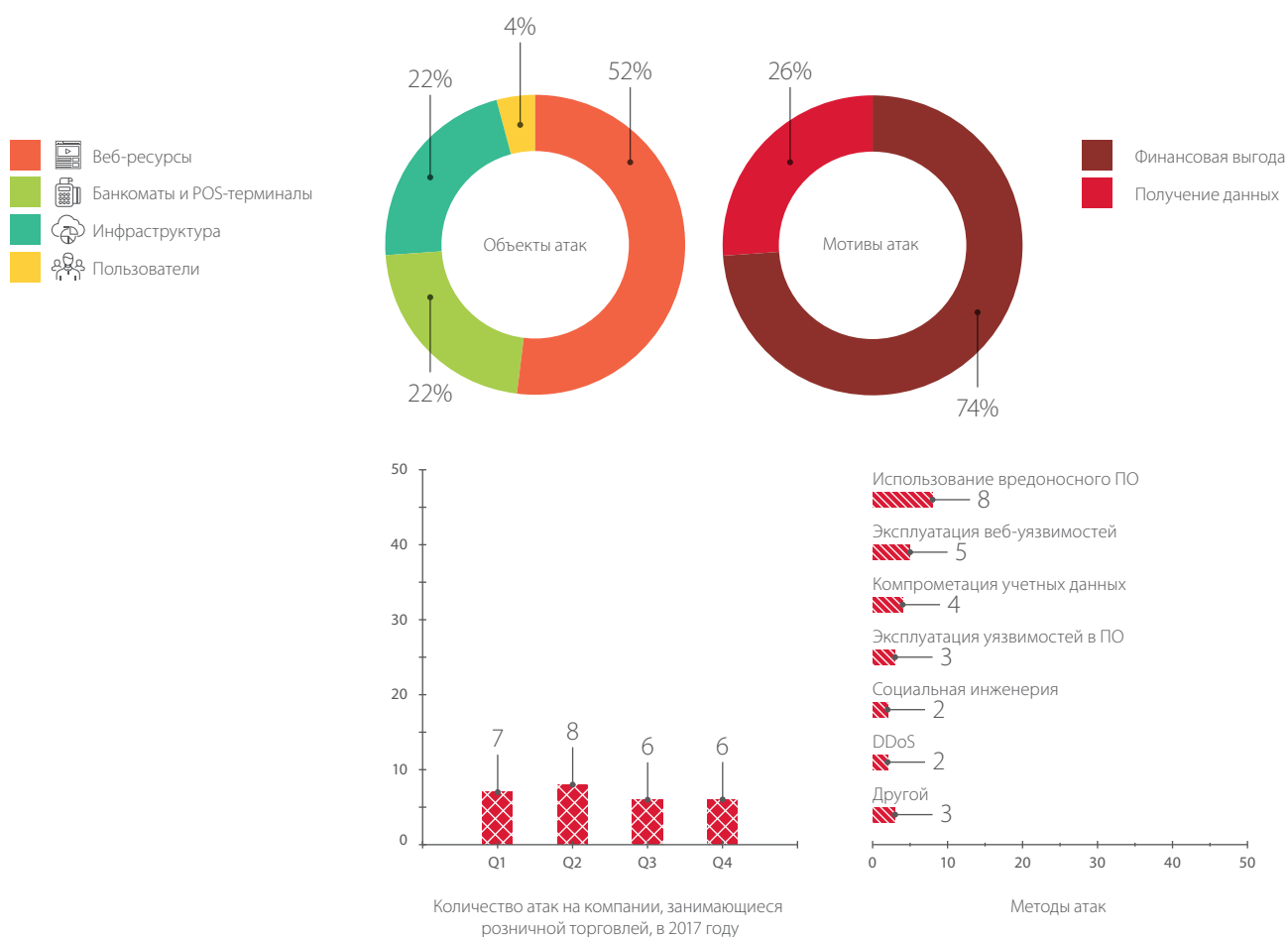
## Промышленные компании



Более половины всех атак на промышленные компании это тщательно спланированные целенаправленные действия целых группировок. Чаще всего такие атаки начинаются с фишинговых рассылок в адрес сотрудников и продолжаются проникновением в инфраструктуру организации и получением контроля над IT-ресурсами. В случае, когда целью злоумышленников является сбор информации, они могут скрытно присутствовать в системе в течение нескольких лет и все это время быть в курсе происходящего в компании.

В 2017 году мы отметили, что вредоносное ПО, нацеленное на промышленность, совершенствовалось и настраивалось под специфику инфраструктуры этих компаний. И этот факт должен настораживать организации, ведь если индустриальные компании не поторопятся обновить используемые ОС и ПО, а также не примут другие необходимые меры защиты, то не исключено, что в следующем году нас ждут громкие целенаправленные атаки с использованием специализированного вредоносного ПО.

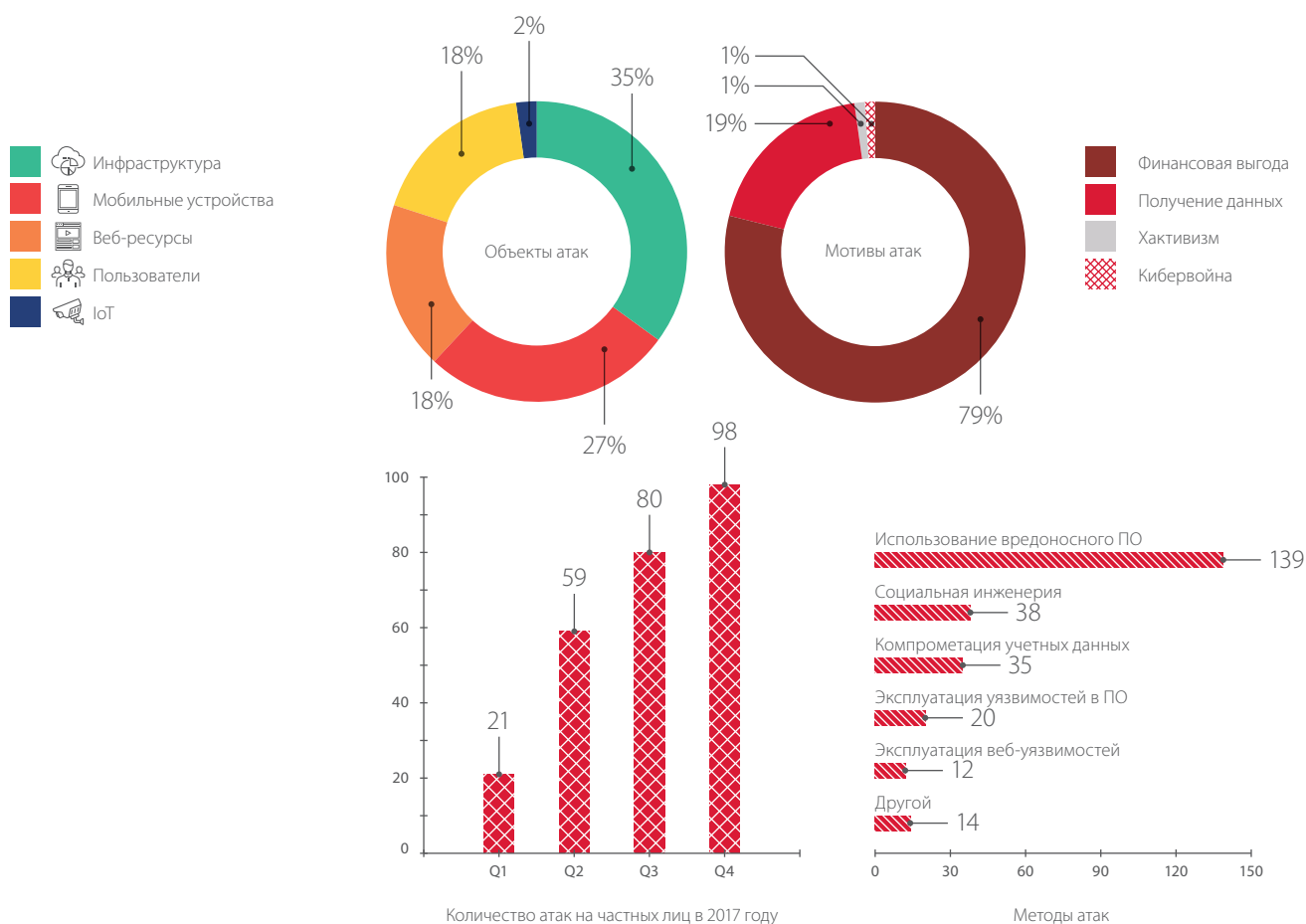
## Розничная торговля



В сфере розничной торговли в 2017 году половина кибератак (52%) была направлена на веб-приложения, преимущественно онлайн-магазины. В ходе таких атак злоумышленники компрометировали учетные данные клиентов, похищали данные их платежных карт, нарушали работу веб-приложений.

Кроме того, почти каждая пятая атака (19%) заключалась во внедрении вредоносного ПО на POS-терминалы, используемые в розничных магазинах. Примечательно, что задача установки трояна на такой терминал совсем не тривиальна. Возможными этапами, на которых злоумышленники пытаются подменить оригинальную прошивку, могут быть завод, транспортировка, сдача в ремонт или обслуживание POS-терминала. Злоумышленники могут вмешаться в процесс обновлений, компрометируя серверы производителей и подменяя оригинальные прошивки. При этом для обычного человека оплата покупки выглядит абсолютно нормально, отличие лишь в том, что вся информация о платежной карте оказывается у злоумышленника.

## Частные лица



Каждая четвертая кибератака в 2017 году была направлена на обычных людей, причем в течение года мы отметили существенный рост этой категории атак. Злоумышленники в атаках на частных лиц предпочитали использовать вредоносное ПО и социальную инженерию. Учитывая, что компьютерная грамотность и осведомленность людей в вопросах информационной безопасности растет, злоумышленникам приходилось придумывать все новые сценарии атак.

Как правило, целью киберпреступников в случае атак на частных лиц была финансовая выгода (например, выкуп за разблокировку данных или возврат учетной записи в социальной сети) или кража информации (данных банковских карт, учетных данных от различных сервисов).

Кроме того, из-за популярности криптовалюты злоумышленников заинтересовали вычислительные мощности персональных компьютеров и мобильных телефонов. Причем помимо распространения троянов и создания целых ботнетов, генерирующих криптовалюту, скрипты для майнинга стали специально встраивать в веб-приложения для того, чтобы заработать. В таких случаях генерация криптовалюты производилась непосредственно в браузере пользователя во время посещения сайта.

## ПРОГНОЗЫ

Подводя итоги 2017 года, можно сделать следующие прогнозы:

- + Масштабные вредоносные атаки будут продолжаться и эволюционировать. При этом они будут нацелены не только на получение прибыли, но и на деструктивное воздействие, в том числе на вывод из строя инфраструктуры целевой организации (или целого ряда компаний отдельной отрасли). Вредоносное ПО превращается в настоящее оружие, способное привести к разрушительным последствиям.
- + Вероятно, что тестирование модели ransomware as a service на частных лицах закончится и злоумышленники перейдут к атакам на компании. Кроме того, подростки, покупающие или скачивающие в интернете вредоносное ПО, а затем попадающие в руки правоохранительных органов, начнут уметь и будут пытаться действовать более скрытно. При этом в интернете появится больше инструкций и обучающих материалов на тему того, какие правила нужно соблюдать, чтобы не угодить в тюрьму.
- + Кибератаки станут еще более запутанными и сложными, в том числе из-за использования взломанных веб-приложений в качестве инструментов атаки, а также многоэтапных кампаний, затрагивающих не только целевую организацию, но и ее партнеров.
- + Если промышленные компании не поторопятся обновить используемые ОС и ПО, а также не примут другие необходимые меры защиты, то мы не исключаем, что в следующем году нас ждут громкие целенаправленные атаки с использованием специализированного вредоносного ПО на промышленность и, в частности, на АСУ ТП.
- + Пока для проведения транзакций банки будут использовать платежные карты, нарушители продолжат применять свои познания в принципах обработки платежных карт, похищая данные и зарабатывая на этом деньги. Вредоносное ПО для POS-терминалов и банкоматов продолжит развиваться, но вместе с этим будут развиваться и средства защиты.
- + Атаки на ICO продолжатся, но если компании до проведения ICO будут больше внимания уделять вопросам безопасности и привлекать специалистов для анализа смарт-контрактов и комплексной защиты инфраструктуры, то ущерб от кибератак станет существенно ниже.
- + Майнинг криптовалюты за счет посетителей веб-сайтов может стать популярней, чем монетизация с помощью контекстной рекламы. Сервисы, предлагающие владельцам сайтов зарабатывать за счет встраивания скриптов для майнинга в код ресурса, уже существуют, и количество их клиентов будет расти.
- + Поскольку в течение 2017 года росло количество новых ботнетов и увеличивался состав существующих, в ближайшее время можно ожидать новых масштабных DDoS-атак, в том числе с использованием уже известного вредоносного ПО.
- + Странам, не регулирующим финансовые операции, связанные с криптовалютой, стоит пересмотреть свои подходы. Без контроля криптовалюты на государственном уровне будет сложно противостоять обогащению злоумышленников, использующих криптовалюту для безнаказанного отмывания денег благодаря ее анонимности.
- + В 2018 году в России пройдут президентские выборы и чемпионат мира по футболу. Такие значимые события вряд ли останутся без внимания киберпреступников. Поскольку в организации этих мероприятий задействовано множество компаний из различных отраслей, мы настоятельно рекомендуем им заранее проверить безопасность и убедиться, что попытки кибератак не смогут сорвать выборы или сказаться на их результатах, а также причинить какие-либо неудобства гостям чемпионата.

## О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.