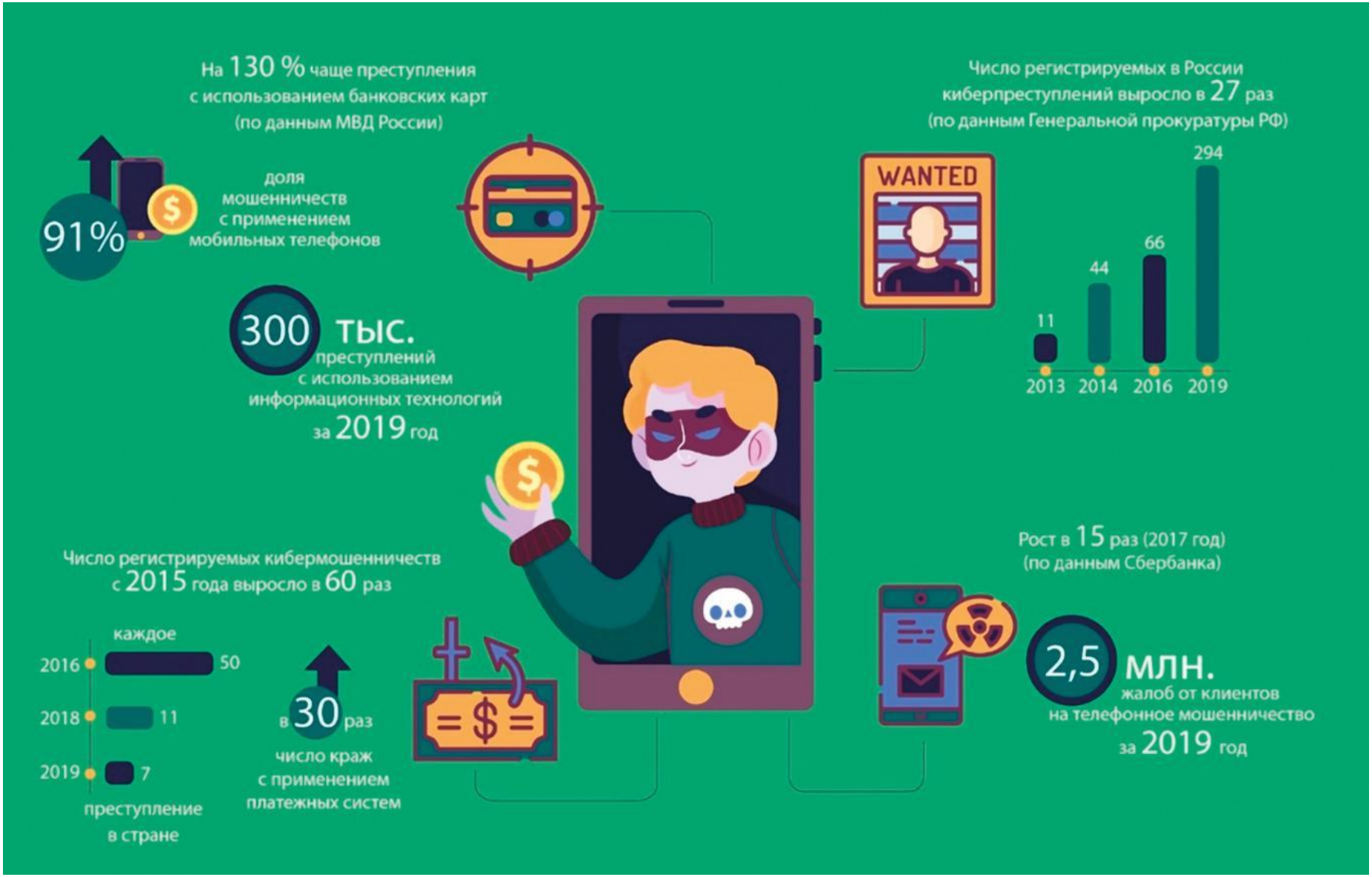
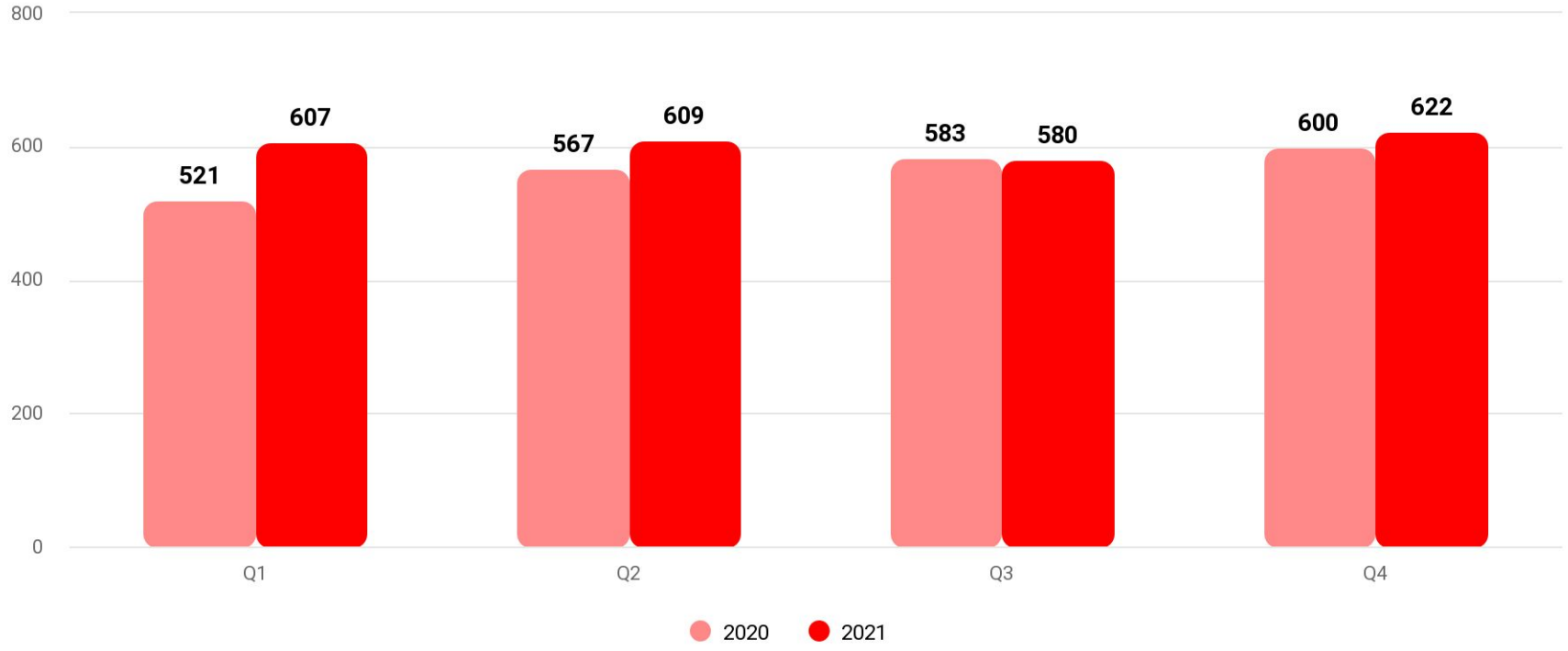
Лекция №1 Определение информационной безопасности. Классификация угроз безопасности. Правовое регулирование информационной безопасности

Индустрия киберпреступности



Количество атак в 2021 году увеличилось всего на 6,5% по сравнению с 2020 годом. О замедлении роста числа атак сообщают и в МВД России. Это связано с тем, что мир адаптировался к новым условиям работы на фоне пандемии коронавируса, а атаки на крупные компании мотивировали топ-менеджеров обращать больше внимания на вопросы, связанные с безопасностью.



Количество атак в 2020 и 2021 годах

Защита информации — комплекс технических, организационных и юридических мер, направленных на обеспечение целостности информации, на обеспечение возможности передать информацию, реализацию права на доступ к информации и множество других целей.

Комплекс технических мер: набор программ, алгоритмов, технических средств, средств проверки прав доступа, как в компьютере, так и физически (замки, сейфы, ключи).

Административные меры: меры на уровне предприятия, которое тоже организует разделение прав доступа к информации (бухгалтер имеет доступ к счетам, директор — ко всему)

Юридические меры: меры, которые обеспечивает государство или другой правоустанавливающий орган для того, чтобы эффективно защищать информацию. Сюда можно отнести различные законы устанавливающие ответственность за нарушение режимов доступа к личной информации (закон о сохранении частной жизни, режим доступа к именам, паспортам, медицинским данным). Гражданский и уголовный кодекс, устанавливающий административную и уголовную ответственность (например за нарушение функционирования сети Интернет, за взлом программ, за взлом сайтов

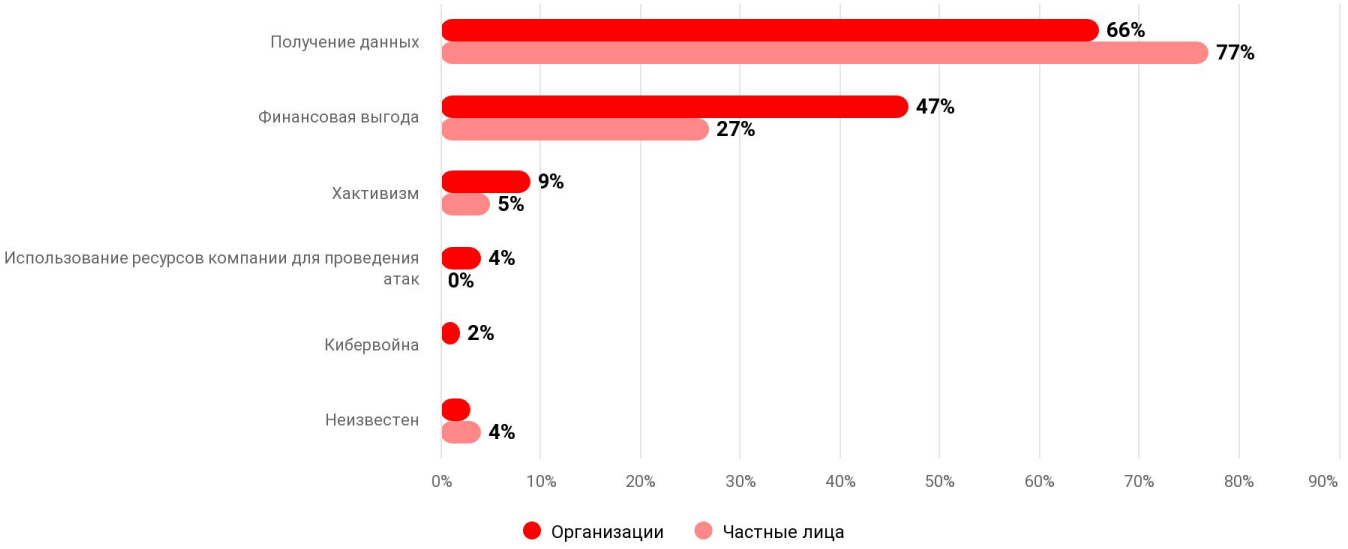
Комплекс мер по защите должны обеспечивать:

Конфиденциальность информации (злоумышленник не должен иметь возможность прочитать информацию).

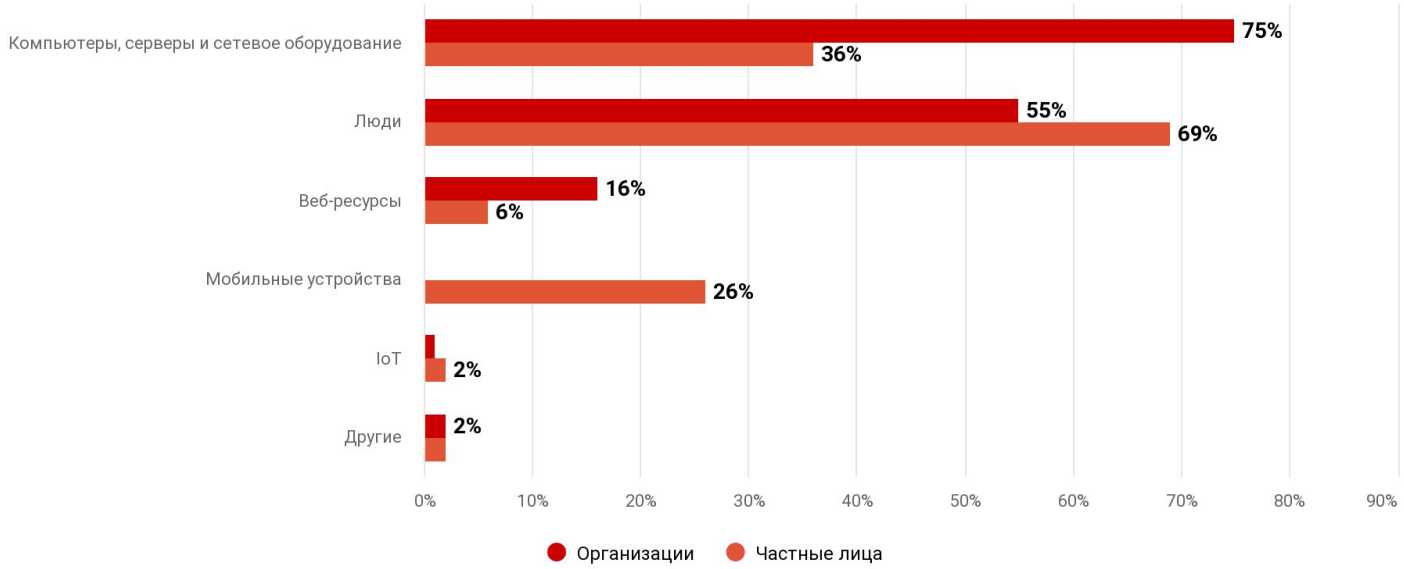
Защиту целостности информации (злоумышленник не должен иметь возможность поменять информацию, даже если она передаётся по открытым каналам связи).

Защиту возможности доступа к информации (злоумышленник не должен иметь возможность сделать так, что легальный пользователь не сможет передать информацию (DDOS, блокировка телевизионного сигнала, нарушение работы радиостанции), попытки прекратить доступ к информации тоже являются уголовным делом)

Мотивы злоумышленников



Объекты атак



Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.
Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Придерживаясь принятой классификации, будем разделять все источники угроз на **внешние и внутренние**.

В свою очередь все угрозы бывают **умышленные или не умышленные**.

Все источники угроз безопасности информации можно разделить на три основные группы:
Обусловленные действиями субъекта (**антропогенные источники угроз**).
Обусловленные техническими средствами (**техногенные источники угрозы**).
Обусловленные **стихийными источниками**.

В качестве **антропогенного источника угроз** можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние так и внутренние

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

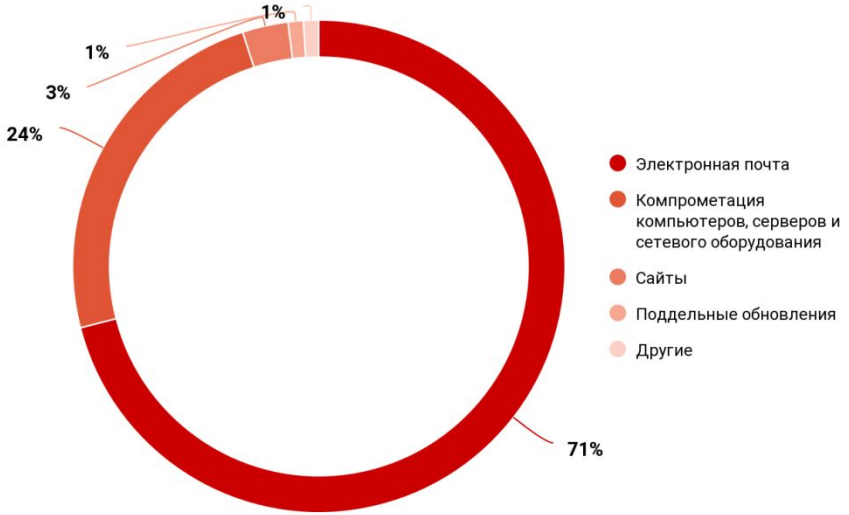
- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

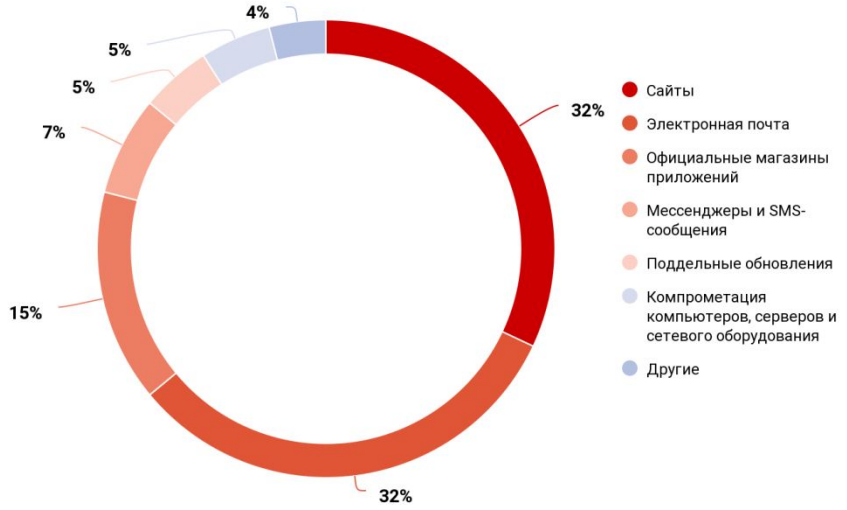
Инициаторы внутренних инцидентов

	1-е полугодие 2019	2-е полугодие 2019	1-е полугодие 2020	2-е полугодие 2020
Прочие внутренние пользователи	55,6%	54,5%	60,1%	62,4%
Внутренние штатные администраторы	27,2%	27,3%	20,7%	20,0%
Аутсорсеры, контрагенты, подрядчики	17,2%	18,2%	19,2%	17,6%

Направления внутренних атак

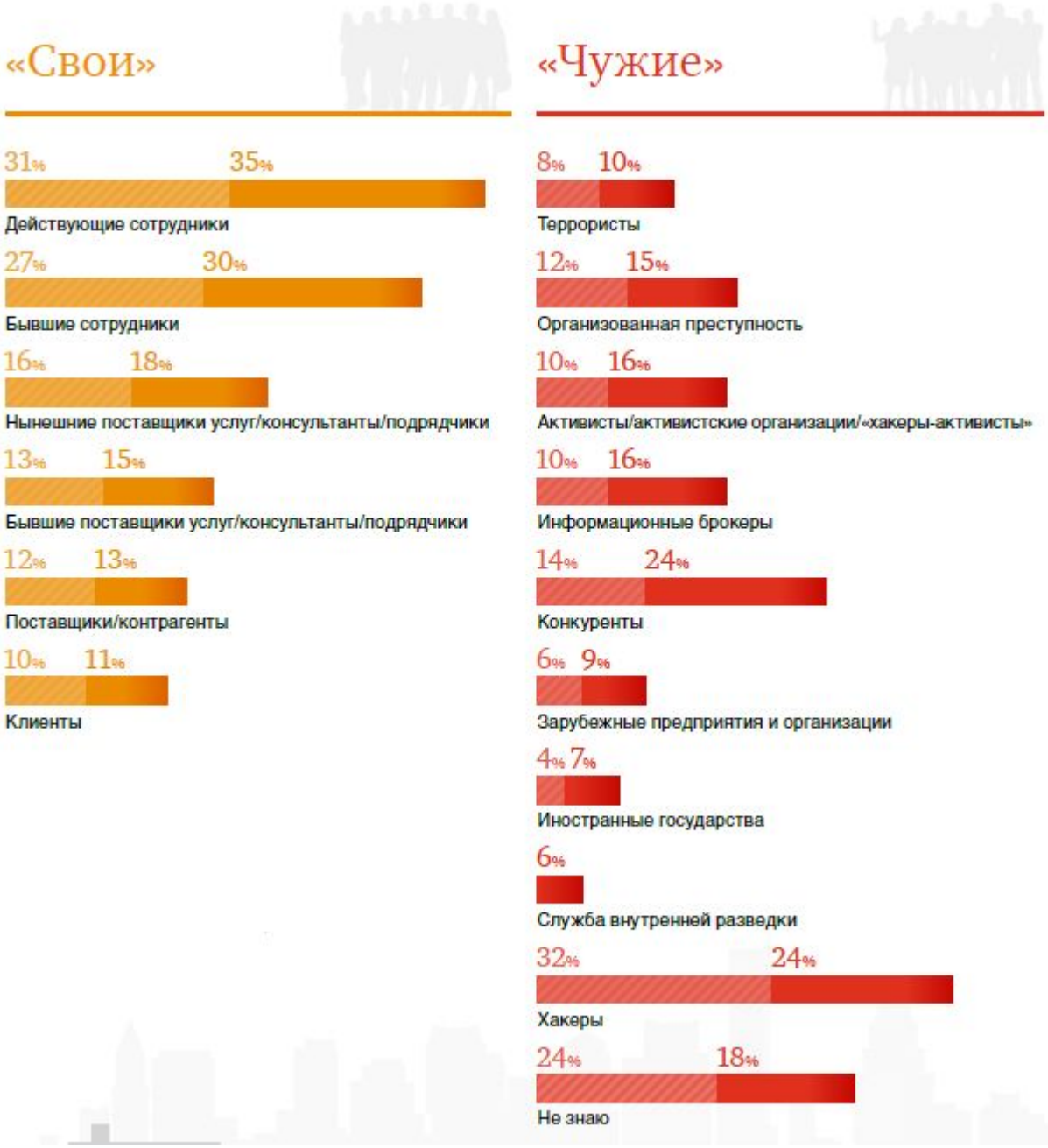
Каналы утечки информации



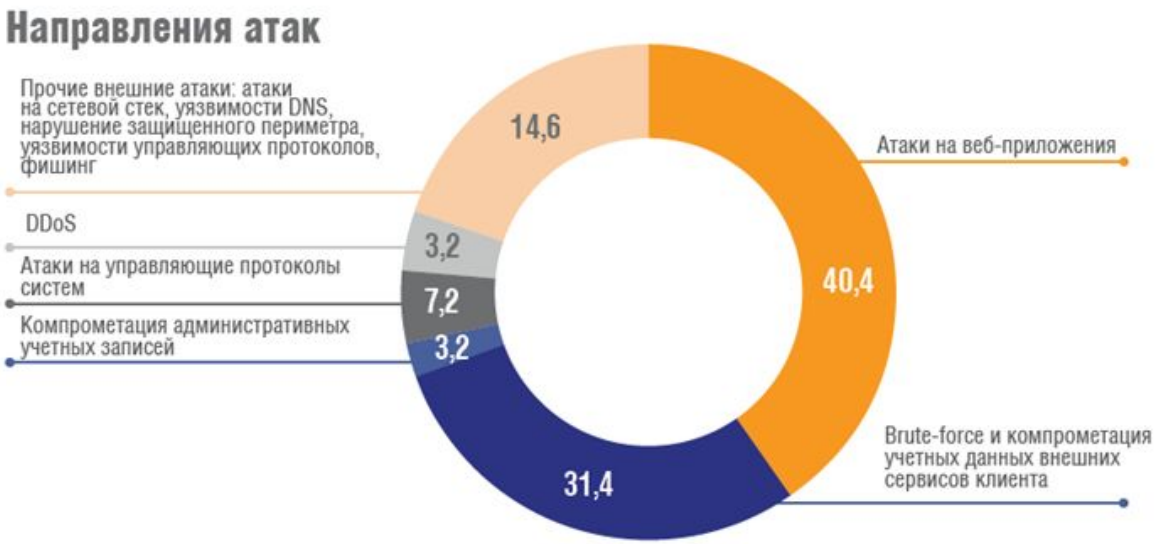


Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

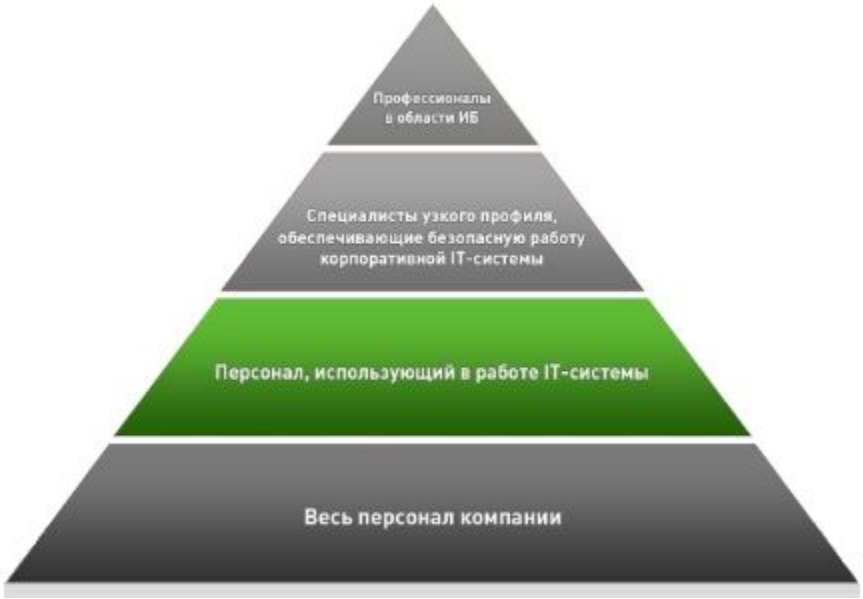
- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков телематических услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур



Направления внешних атак



Уровень осведомленности пользователей в вопросах ИБ




Каждый 4-ый
пользователь оставляет злоумышленникам возможность проникнуть в корпоративную сеть
МОЙ ПАРОЛЬ 1234567
1/3
пользователей хранит пароли в легкодоступном месте
Каждый 2-ой
пользователь не знаком с правилами информационной безопасности
2 из 3
пользователей посещают потенциально опасные сайты с рабочего компьютера
Каждый 3-ий
работник постоянно использует один и тот же пароль
ПАРОЛЬ


8 из10
работников компании допускают утечку корпоративной информации
37%
работников используют рабочую почту в личных целях
85% дают злоумышленникам возможность взлома корпоративной сети посредством e-mail
15%
работников компании готовы передать третьим лицам конфиденциальну ю информацию компании
ИНФОРМАЦИЯ
TOP SECRET
более 60%
мобильных телефонов не защищены паролем

Вторая группа содержит источники угроз, определяемые **технократической деятельностью** человека и развитием цивилизации. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания.

Технические средства, являющиеся источниками потенциальных угроз безопасности информации так же могут быть **внешними**:

- средства связи;
- сети инженерных коммуникации (водоснабжения, канализации);
- транспорт.

и **внутренними** :

- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные средства (охраны, сигнализации, телефонии);

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех.

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы:

- пожары;
- землетрясения;
- наводнения;
- ураганы;
- различные непредвиденные обстоятельства;
- необъяснимые явления;
- другие форс-мажорные обстоятельства

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации**: информационные, программные, физические, радиоэлектронные и организационно–правовые**

К информационным угрозам относятся:
несанкционированный доступ к информационным ресурсам;
незаконное копирование данных в информационных системах;
хищение информации из библиотек, архивов, банков и баз данных;
нарушение технологии обработки информации;
противозаконный сбор и использование информации;
использование информационного оружия.

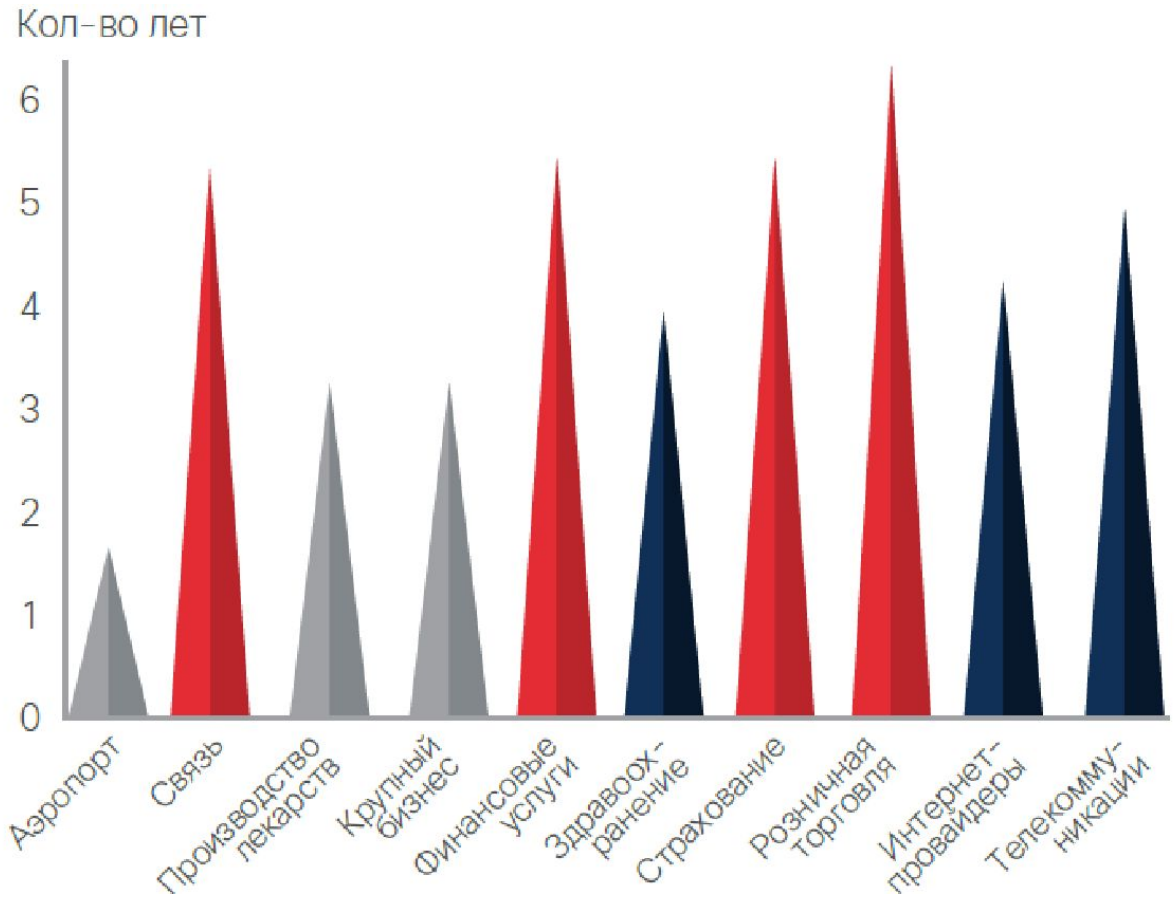
К физическим угрозам относятся:
уничтожение или разрушение средств обработки информации и связи;
хищение носителей информации;
хищение программных или аппаратных ключей и средств криптографической защиты данных;
воздействие на персонал

К программным угрозам относятся:
использование ошибок и "дыр" в ПО;
компьютерные вирусы и вредоносные программы;
установка "закладных" устройств

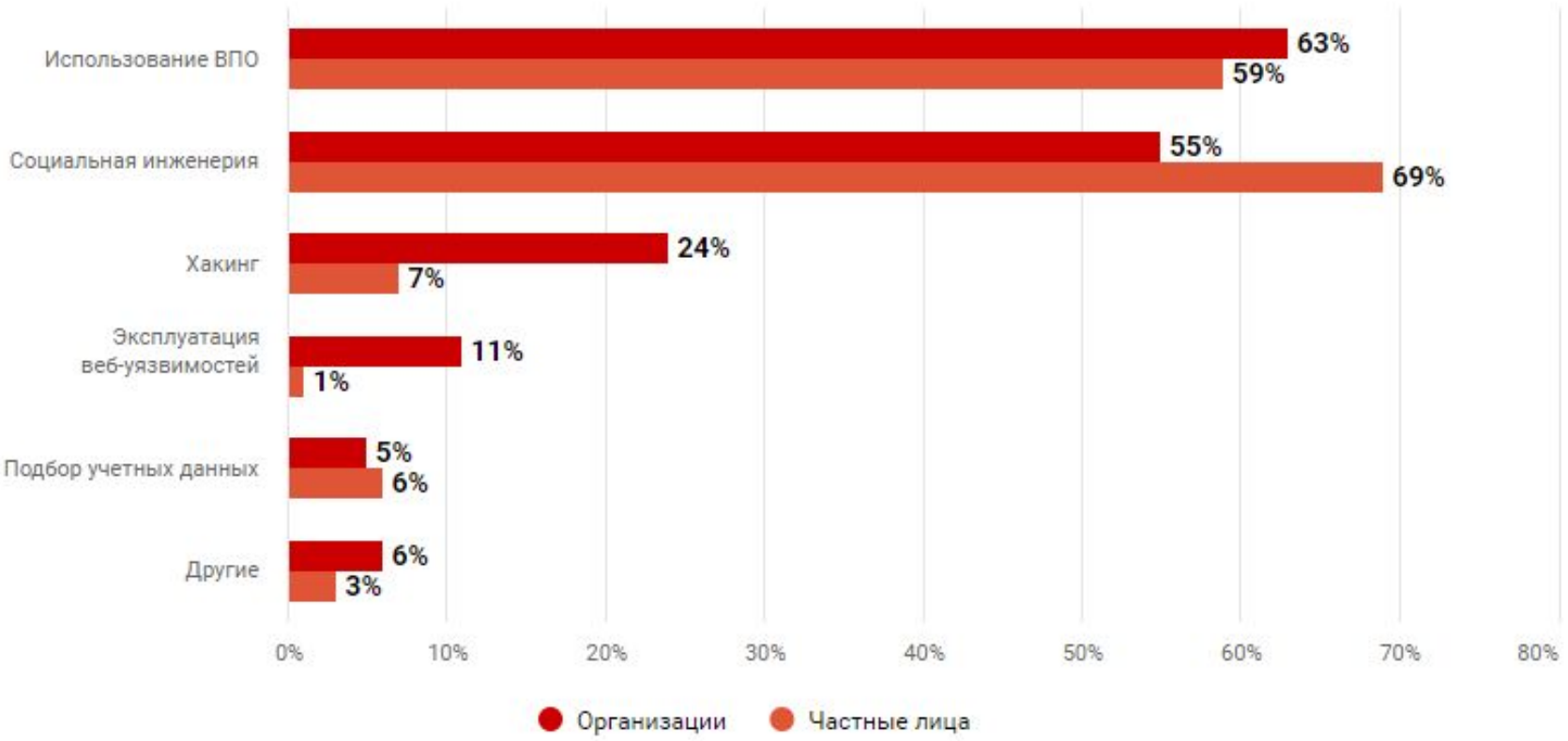
К радиоэлектронным угрозам относятся:
внедрение электронных устройств перехвата информации в технические средства и помещения; перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К организационно–правовым угрозам относятся:
закупки несовершенных или устаревших информационных технологий и средств информатизации; нарушение требований законодательства и задержка в принятии необходимых нормативно–правовых решений в информационной сфере.

Средний возраст программного обеспечения в организациях



Популярные методы атак



Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Федеральная служба охраны Российской Федерации (ФСО России);
- Служба внешней разведки Российской Федерации (СВР России);
- Министерство обороны Российской Федерации (Минобороны России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Международный стандарт «Общие критерии оценки защищённости информационных технологий» (ISO/IEC 15408) описывает инфраструктуру (framework), в которой *потребители* компьютерной системы могут описать требования, *разработчики* могут заявить о свойствах безопасности продуктов, а *эксперты* по безопасности определить, удовлетворяет ли продукт заявлениям. Таким образом, ISO/IEC 15408 позволяет обеспечить условия, в которых процесс описания, разработки и проверки продукта будет произведён с необходимой скрупулёзностью

Федеральный закон Российской Федерации «О персональных данных» от 27 июля 2006 года № 152-ФЗ регулирует деятельность физических и юридических лиц по обработке и использованию персональных данных. Закон «О персональных данных» требования и правила по защите персональных данных ко всем организациям, государственным и частным компаниям, которые хранят, обрабатывают и собирают персональные данные своих сотрудников, посетителей или клиентов.

Закон «О связи» и приказ Министерства связи № 2339 от 9 августа 2000 г и Приказ Министерства информационных технологий и связи РФ от 16 января 2008 г. N 6 "Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий.

СОРМ (сокр. от *Система технических средств для обеспечения функций оперативно-розыскных мероприятий*) — комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи. Операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами

31 июля 2014 года премьер-министр РФ Дмитрий Медведев подписал **постановление правительства №743**, по которому соцсети, форумы и любые сайты для общения, доступные всем пользователям интернета должны подключать оборудование и ПО для силовиков согласно плану мероприятий, разработанных ФСБ. С помощью этого спецслужбы смогут в автоматическом режиме получать информацию о действиях пользователей этих сайтов, схема работает аналогично СОРМ.

Закон «Об информации, информатизации и защите информации» 149-ФЗ

В законе выделены следующие **цели защиты информации**:

- Предотвращение утечки, хищения, утраты, искажения информации
- Предотвращения угроз безопасности личности, общества, государства
- Предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации
- Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных
- Сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством
- Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем

Федеральный закон № 398-ФЗ от 28 декабря 2012 года (закон о блокировке экстремистских сайтов) «Законопроект Лугового»

Закон позволяет Роскомнадзору по предписанию Генпрокуратуры РФ производить немедленную блокировку без решения суда сайтов, распространяющих призывы к массовым беспорядкам и с другой экстремистской информацией. Вступил в силу 1 февраля 2014 года

Федеральный закон от 2 июля 2013 года № 187-ФЗ «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях»

закон, подразумевающий возможность блокировки сайтов, содержащих нелицензионный контент, по требованию правообладателя. Изначально предполагалось, что это коснётся всех видов информации, однако, после внесения поправок, закон будет применяться только для видеопродукции. Если после предупреждения владельцы сайта не удалят спорный материал, то весь ресурс будет блокироваться. Однако, правообладатель должен будет доказать, что обладает правами в отношении того размещённого в сети контента, который он намеревается удалить

Федеральный закон № 97-ФЗ от 5 мая 2014 года «О внесении изменений в Федеральный закон „Об информации, информационных технологиях и о защите информации“, также известный как «Закон о блогерах»

российский федеральный закон, обязывающий авторов интернет-ресурсов (сайтов, блогов и пр.) с аудиторией «свыше 3000 пользователей в сутки» регистрироваться в Роскомнадзоре и накладывающий ряд ограничений на содержимое этих ресурсов

Закон определяет блог как любой сайт или страницу в Сети. Его владелец не только сам обязан соблюдать законодательство Российской Федерации, но и следить, чтобы его не нарушали пользователи ресурса, например, оставляющие комментарии

Федеральный закон № 139-ФЗ от 28 июля 2012 года
О внесении изменений в Федеральный закон „О защите детей от информации, причиняющей вред их здоровью и развитию“ и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет». Этот закон внёс в другие федеральные законы ряд положений, предполагающих фильтрацию интернет-сайтов по системе чёрного списка и блокировку запрещённых интернет-ресурсов

Закон «О лицензировании отдельных видов деятельности»
Закон №128-ФЗ от 8.08.2001 устанавливает требование к обязательному лицензированию некоторых видов деятельности, в том числе, относящихся к информационной безопасности:

- Распространение шифровальных (криптографических) средств;
- Техническое обслуживание шифровальных средств;
- Предоставление услуг в области шифрования информации;
- Разработка и производство шифровальных средств, защищенных с их помощью информационных систем и телекоммуникационных систем
- Выдача сертификатов ключей ЭЦП, регистрация владельцев ЭЦП
- Выявление электронных устройств, предназначенных для негласного получения информации
- Разработка и производство средств защиты конфиденциальной информации
- Техническая защита конфиденциальной информации

Закон 63-ФЗ «Об электронной подписи»
Закон «Об электронной подписи» обеспечивает правовые условия использования электронной цифровой подписи в электронных документах. Действие данного закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок

Федеральный закон «О связи» № 126-ФЗ от 07.07.2003г. в редакции от 21.07.2014г., а также Постановления Правительства РФ № 758 от 31 июля 2014г. и № 801 от 12 августа 2014г., которые внесли изменения в «Правила оказания услуг связи по передаче данных». Постановление запрещает анонимный бесплатный Wi-Fi доступ.

Президент России Владимир Путин подписал **пакет поправок к законодательству, которые запрещают использование средств для обхода блокировок**. Об этом говорится на официальном интернет-портале правовой информации.

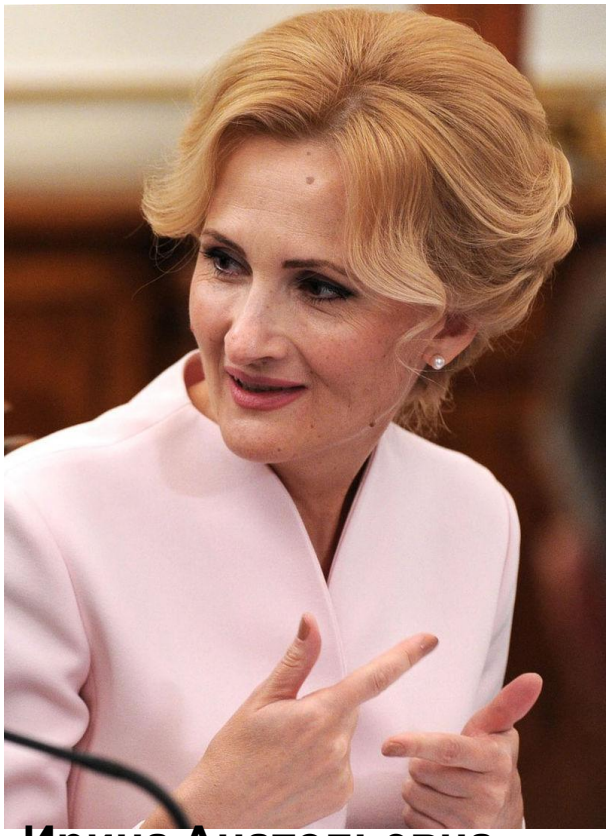
Пакет поправок был принят Госдумой 21 июля, а 25 июля получил одобрение Совета Федерации. Согласно поправкам, ФСБ и МВД получат полномочия находить сервисы, которые помогают получать доступ к заблокированным в России сайтам. В случае, если владельцы таких сервисов не запретят доступ к запрещенной в России информации, то сервисы будут заблокированы. Запрет анонимайзеров, VPN и других средств, помогающих обходить блокировки сайтов в России, **вступит в силу с ноября 2017 года**.

Закон Яровой (или пакет Яровой) — федеральный закон Российской Федерации от 06.07.2016 № 374-ФЗ о внесении изменений в закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

Пакет Яровой» состоит из двух законопроектов:

- № 1039101-6 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»
- № 1039149-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»

Второй законопроект обязывает операторов связи хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев) в соответствии с 64-ой статьей федерального закона "О связи", а информацию о фактах приема, передачи, доставки и обработки сообщений и звонков — 3 год



Ирина Анатольевна Яровая

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) — федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности

Деятельность ФСТЭК решает следующие вопросы:

- обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;
- противодействия иностранным техническим разведкам на территории Российской Федерации;
- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения её утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях её добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- осуществления экспортного контроля

Банк данных угроз безопасности: http://bdu.fstec.ru/threat

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) — федеральный орган исполнительной власти России в ведении Минкомсвязи России. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

Единый реестр доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено, — автоматизированная информационная система ведения и использования базы данных о сайтах, содержащих запрещённую к распространению в России информацию
http://eais.rkn.gov.ru/

Елена Борисовна Мизулина

лига безопасного интернета

http://ligainternet.ru/

Управление К – одно из подразделений Министерства внутренних дел, которое противодействует преступлениям в области информационной безопасности, а также незаконному обороту радиоэлектронных средств и специальных технических средств

В обязанности представителей Управления К входит

- борьба с нарушением авторских и смежных прав
- выявление и пресечение фактов неправомерного доступа к компьютерной информации
- борьба с распространителями вредоносных программ
- выявление нарушений правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных выявление использования подложных банковских карт
- борьба с распространением порнографии посредством сети Интернет и компакт-дисков
- выявление незаконного подключения к телефонным линиям
- борьба с незаконным оборотом радиоэлектронных (РЭС) и специальных технических средств (СТС)
- противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей включая сеть Интернет