ROOT LEVEL RESOURCES

ДОРОЖНАЯ КАРТА ПРОВАЙДЕРА СЕТЕВОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В настоящее время развитие полноценного общества не представляется без использования информационно-телекоммуникационных технологий, в результате чего неизбежно происходит увеличение количества преступлений в этой сфере.

По данным ФКУ «Главного информационно-аналитического центра» Министерства внутренних дел Российской Федерации: в январе - сентябре 2019 года зарегистрировано **205,1 тыс. преступлений**, совершенных с использованием информационно-телекоммуникационных технологий, или на 69,2% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,1% в январе - сентябре 2018 года до 13,5%.

Практически все такие преступления (98,3%) выявляются органами внутренних дел.

Почти половина таких преступлений (48,3%) относятся к категориям тяжких и особо тяжких: 99,0 тыс. (+169,9%); больше половины (52,9%) совершается с использованием сети «Интернет»: 108,5 тыс. (+43,9%), больше трети (38,3%) – средств мобильной связи: 78,5 тыс. (+90,7%).

Три четверти таких преступлений (78,6%) совершается путем кражи или мошенничества: 161,3 тыс. (+84,9%), почти каждое одиннадцатое (8,7%) – с целью незаконного производства, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов: 17,9 тыс. (+34,7%).

Генпрокуратура РФ характеризует рост киберпреступности как «весьма существенный». Если сравнивать с данными, которые ведомство приводит для других видов преступлений, темпы роста в этом сегменте оказываются самыми высокими.

Всего зарегистрированных преступлений в январе-сентябре 2019:

205 116

Из них тяжких и особо тяжких

99 040

В том числе совершенных с использованием или применением:

23 259 Расчетных (пластиковых) карт	**726** Фиктивных электронных платежей
14 267 Компьютерной техники	**108 540** Сети «Интернет»
4 494 Программных средств	**78 479** Средств мобильной связи

158 УК РФ – Кража	**61 074**
159 УК РФ – Мошенничество	**83 333**
159³ УК РФ – Мошенничество с использованием платежных карт	**10 371**
159⁶ УК РФ – Мошенничество в сфере компьютерной информации	**533**
171² УК РФ – Незаконные организация и проведение азартных игр	**685**
205² УК РФ – Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма	**161**
228¹ УК РФ – Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо из частей, содержащих наркотические средства или психотропные вещества	**17 871**
242, 242¹, 242² УК РФ – Изготовление порнографических материалов	**1 485**
280 УК РФ – Публичные призывы к осуществлению экстремистской деятельности	**210**
Преступления в сфере компьютерной информации глава **28 УК РФ**	**2 044**
272 УК РФ – Неправомерные доступ к компьютерной информации	**1 683**
273 УК РФ – Создание, использование и распространение вредоносных компьютерных программ	**354**
274 УК РФ – Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	**–**
274¹ УК РФ – Неправомерное воздействие на критическую информационную инфраструктуру РФ	**–**

ROOT LEVEL RESOURCES

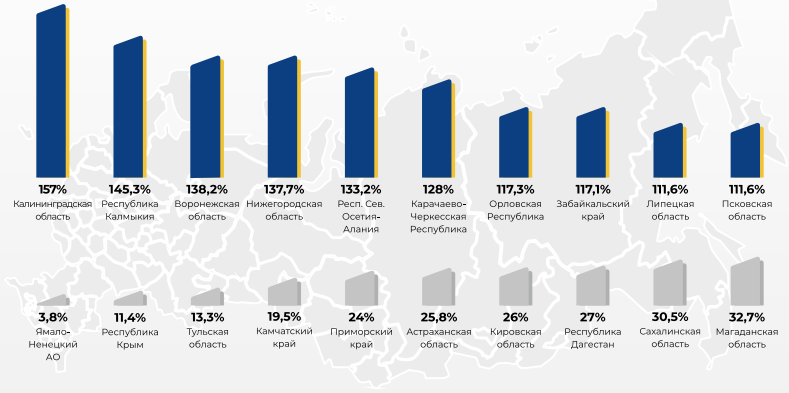
Всего нераскрытых преступлений в отчетном периоде:

Всего раскрытых преступлений в отчетном периоде:

Всего уголовных дел которые направлены в суд с обвинительных заключением, обвинительных актом, обвинительным постановлением

ROOT LEVEL RESOURCES

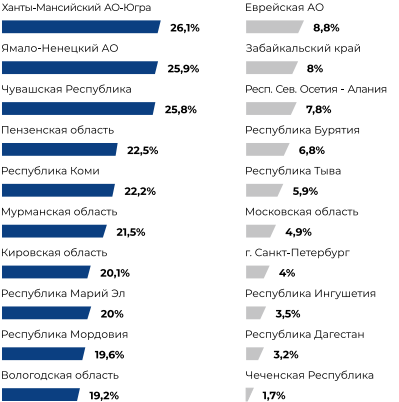
Регионы Российской Федерации с наибольшими и наименьшими темпами прироста зарегистрированных преступлений



Удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий (в общей структуре преступности)

ROOT LEVEL RESOURCES

Регионы Российской Федерации с наибольшим и наименьшим удельным весом преступлений



Регионы Российской Федерации с наибольшей и наименьшей раскрываемостью преступлений

Киберпреступник в Российской Федерации – кто он?

Сегодня провести кибератаку может едва ли не каждый. Тем не менее, нынешний киберпреступник — это в большинстве случаев группировка; одиночек, организующих атаку самостоятельно от начала и до конца, практически нет. Атаки стали сложнее, и злоумышленникам необходимо кооперироваться. Успешный киберпреступник сегодня — это хороший управленец, который набрал команду, а сам, возможно, вообще не является программистом. Это значительно затрудняет атрибуцию атак при их расследовании, а также увеличивает общее число вовлеченных в киберкриминальную деятельность субъектов. Тем не менее, на основе конвергенции знаний юридических наук и статистических данных, можно составить ориентировочный социальный портрет киберпреступника:

Киберпреступник в Российской Федерации – кто он?

ROOT LEVEL RESOURCES

1 По образованию:

Образовательный уровень лиц, совершающих данную категорию преступлений, является важным показателем интеллектуального уровня преступников и находится в определенной взаимосвязи с характером их преступных действий.

Считается, что компьютерные преступники — высококвалифицированные специалисты с высшим техническим или юридическим образованием. Однако анализ судебно-следственной практики показал что образование у киберпреступников в основном техническое среднее, незаконченное высшее или высшее, а среднее специальное встречалось реже. В криминологической литературе можно встретить упоминание киберпреступников как людей любознательных, талантливых и имеющих высокий уровень интеллекта, склонных к самообразованию. Однако следует иметь в виду, что в совершение компьютерных преступлений втянут довольно широкий круг лиц, среди которых встречаются как дилетанты, так и высококвалифицированные специалисты, т.е. портрет типичных преступников неоднороден.

Самую немногочисленную долю раскрытых преступлений в сфере компьютерных технологий составляют наиболее опасные преступления, совершаемые высококвалифицированными специалистами в области высоких технологий. Во многом это связано с тем, что непрофессионалам, как правило, не хватает знаний, навыков и технического обеспечения для эффективного сокрытия преступлений.

2 По возрасту:

Возраст у компьютерных преступников в основном от 18 до 35 лет. Более старший возраст встречается реже, так как компьютерная техника в РФ стала широко использоваться только в конце 90-х гг., а немолодым людям ее освоить сложнее. В настоящее время происходит омоложение компьютерной преступности, так как сейчас дети и подростки с ранних лет связаны с компьютерной техникой и сетевыми информационными технологиями. По мнению ряда ученых, возраст компьютерных преступников в основном колеблется от 15 до 45 лет.

3 Пол:

Большинство ученых сходятся во мнении, что совершение преступлений рассматриваемой категории характерно для мужчин. Однако в последнее время наблюдается тенденция к увеличению количества женщин, совершающих данные преступления. При этом женщины обычно выступают в качестве соучастников преступления наряду с мужчинами.

Киберпреступник в Российской Федерации – кто он?

ROOT LEVEL RESOURCES

4 Мотив:

Наиболее характерными мотивами лиц, совершающих компьютерные преступления, можно считать:

- Корыстные
- Хулиганские
- Политические
- Игровые
- Исследовательский интерес
- Потребность в самоутверждении
- Месть
- Мотивы, связанные с психическими отклонениями
- Самоутверждение
- Жажда славы.

5 Внешность и психологические аспекты личности:

Как правило, это:

- Человек, не обладающий привлекательными внешними данными или имеющий трудности общения со сверстниками, противоположным полом, ищущий самореализацию в виртуальном мире, достигая при этом определенных профессиональных высот в программировании и использовании электронной цифровой информации.
- Замкнутый, скрытный.
- Стремящийся к самоутверждению, желающий получить известность, приобрести авторитет в своем кругу.
- Является яркой, мыслящей личностью, способной принимать ответственные решения.
- У них часто наблюдается завышенная самооценка, а также правовой нигилизм, несмотря на который они не имеют преступного прошлого.
- Компьютерная система и информационно-компьютерные технологии составляют смысл их жизни.
- Имеют психические отклонения, связанные с фанатичным отношением к компьютерной технике и технологиям.

Однако стоит отметить, что сейчас быть киберпреступником модно прежде всего из-за того, что выгодно в материальном плане. В результате в киберпреступность потянулись предприимчивые, авантюристичные и даже харизматичные люди, которые могут получить крупные преступные доходы, с большой вероятностью избежав при этом уголовной ответственности.

Изучение особенностей личности компьютерных преступников и систематизация полученных знаний — важная криминалистическая задача, которую необходимо осуществлять на регулярной основе в связи с высокой динамикой компьютерной преступности. Это способно не только повлиять на качество раскрытия и расследования таких преступлений, но и оказать помощь в их криминалистическом предупреждении.

Что поставлено на карту?

ROOT LEVEL RESOURCES

Из-за динамично развивающихся информационных технологий виды киберпреступлений видоизменяются, а схемы получения противозаконного заработка с каждым годом становятся все изощреннее. На данный момент можно выделить следующие виды киберпреступлений:

Кража данных

Конкурентный шпионаж, фишинг, хищение интеллектуальной собственности, кража информации, составляющей коммерческую тайну, учетных данных и другой конфиденциальной информации.

Финансовые преступления

Кража криптовалюты, мошенничество в системах онлайн-банкинга и мобильного банкинга, атаки на банкоматы, системы карточного процессинга, SWIFT, платежные шаблоны.

Атаки на критическую инфраструктуру

Атаки на системы водоснабжения, транспортную инфраструктуру, системы управления технологическим процессом в энергетической и нефтегазовой промышленности.

Атаки с использованием вредоносного ПО

Создание, распространение и контроль вредоносных программ, бот-сетей, мошеннические e-mail рассылки, шифровальщики и шпионское ПО.

Информационные войны

Вымогательство, подрыв репутации, распространение негативной информации, преследование и кража личных данных.

Инсайдерские угрозы

Злоупотребление служебными полномочиями, конкурентный шпионаж, утечка данных, кража учетной записи

DDoS-атаки

Заказные и целенаправленные атаки на веб-сервисы с целью приостановления их деятельности или затруднения доступа к ним

Кража интеллектуальной собственности

Присвоение исходного кода, программного обеспечения и других информационных продуктов

Кто следующий в списке? Все под прицелом:

ROOT LEVEL RESOURCES

Киберпреступники часто проводят целевые атаки на предприятия, обрабатывающие или хранящие информацию, которая может быть использована преступниками с целью получения прибыли. Наиболее часто целевым атакам в Российской Федерации подвергаются:

1

Объекты критической информационной инфраструктуры (КИИ). В 2018 году было выявлено 4,3 млрд. кибератак на критическую информационную инфраструктуру РФ. Объектами атак стали компания "Роснефть" и два десятка других крупных российских организаций, в том числе относящихся к таким стратегическим отраслям, как нефтепереработка, газовая и химическая промышленность, сельское хозяйство и т.д. Злоумышленники также пытались атаковать несколько крупных российских бирж.

2

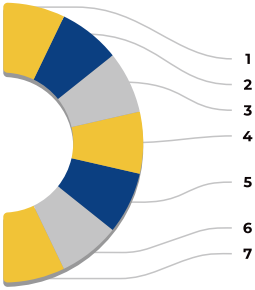
От КИИ стоит отдельно выделить финансово-кредитные организации, особенно банки, которые широко используют информационные технологии. Преступники атакуют серверы или банковскую сеть, чтобы получить доступ к данным и осуществить незаконный перевод средств с банковских счетов пользователей. Однако кража — не самое страшное, что может случиться с финансовой организацией. Банки оказались в числе мишеней для прогосударственных хакерских групп, специализирующихся на диверсиях и саботаже. Одна такая кибератака в случае успеха может привести к ликвидации самой кредитно-финансовой организации и стать одной из причин коллапса финансовой системы целого государства.

3

Биллинговые компании. Когда для атаки выбирается биллинговая компания, преступники пытаются получить доступ к учетным записям пользователей или украсть ценную информацию, такую как клиентские базы данных, финансовую информацию или технические данные.

Почему страховая индустрия не спешит предлагать широкое покрытие по киберстрахованию?

Основной проблемой в России оказывается отсутствие понимания сути данного вида страхования со стороны клиентов, а также неподготовленность со стороны страховых компаний к внедрению данного страхового продукта. Кроме этого стоит выделить:



Специфика российского законодательства:

1. Угрозы роста интенсивности
2. Угрозы концентрации
3. Сложно строить и оценивать модель риска
4. Отсутствие инфраструктуры по определению и урегулированию страховых случаев
5. Недостаток «аппетита к новым рискам» - угроза капиталу компании в случае ошибки
6. Сложный и дорогостоящий андеррайтинг
7. Технические сложности организации (пере)страхования, урегулирования убытков

Что нужно потребителю?

ROOT LEVEL RESOURCES

Упрощение процедуры принятия рисков

Формирование прецедентов и статистики на рынке: начало работы с небольших лимитов

Понятное определения покрытия

Создание простых и понятных продуктов

Рынок киберстрахования в России на данный момент находится на начальном этапе, но со временем он может стать качественным средством обеспечения информационной безопасности и защиты от киберугроз, ведь потенциальный рынок такого страхования огромен, так как любой банк, компания, которая владеет ценными данными и важной информацией, оказываются в зоне риска.

Обзор основ законодательства Российской Федерации, регулирующего вопросы правового обеспечения сетевой безопасности:

ROOT LEVEL RESOURCES

Конституция Российской Федерации от 12.12.1993: http://www.consultant.ru/document/cons_doc_LAW_28399/

Кодифицированные нормативно-правовые акты:

Гражданский кодекс Российской Федерации от 30.11.1994 №51-ФЗ в 4 частях:
1) http://www.consultant.ru/document/cons_doc_LAW_5142/,
2) http://www.consultant.ru/document/cons_doc_LAW_9027/#dst0,
3) http://www.consultant.ru/document/cons_doc_LAW_34154/#dst0,
4) http://www.consultant.ru/document/cons_doc_LAW_64629/#dst0

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_34661/

Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_10699/

Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_34683/

Налоговый кодекс Российской Федерации от 31.07.1998 №146-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_19671/

Федеральные законы Российской Федерации и прочее:

Об информации, информационных технологиях и о защите информации от 27.07.2006 №149-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_61798/

О государственной тайне от 21.07.1993 №5485-1: http://www.consultant.ru/document/cons_doc_LAW_2481/#dst0

О коммерческой тайне от 29.07.2004 №98-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_48699/#dst0

О банках и банковской деятельности от 02.12.1990 №395-1: http://www.consultant.ru/document/cons_doc_LAW_5842/

О страховании вкладов в банках Российской Федерации от 23.11.2003 №177-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_45769/

О лицензировании отдельных видов деятельности от 04.05.20111 №99-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_113658/

О персональных данных от 27.27.2006 №152-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_61801/

О рынке ценных бумаг от 22.04.1996-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_10148/

О связи от 07.07.2009 №126-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_43224/

О техническом регулировании от 27.12.2002 №184-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_40241/

О безопасности критической информационной инфраструктуры Российской Федерации от 26.07.2017 №187-ФЗ: http://www.consultant.ru/document/cons_doc_LAW_220885/

О таможенном регулировании в Российской Федерации от 03.08.2018: http://www.consultant.ru/document/cons_doc_LAW_304093/

Об утверждении Доктрины информационной безопасности Российской Федерации от 05.12.2016 №646: http://www.consultant.ru/document/cons_doc_LAW_208191/

О стратегии национальной безопасности Российской Федерации от 31.12.2015 №683: http://www.consultant.ru/document/cons_doc_LAW_191669/

ГОСТ «34.0003-90. Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. От 27.12.1990 №2299: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=STR&n=10020#007375066912518613