ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Макаревич
ГУПР МВД Республики Беларусь

Статистика

За *2006 г.* выявлено **847** преступлений, совершенных с использованием компьютерной техники, из которых **334** – против информационной безопасности

Только за первое полугодие *2007 г.* выявлено уже **435** преступлений против информационной безопасности, анализ количества преступлений, совершенных в указанный период с использованием компьютерной техники, не производился

Для реальной картины необходимо учитывать:

- неочевидность преступлений
- нежелание пострадавших придавать огласке
- особенности учета преступлений
- особенности правоприменительной практики

Замечания:

- отсутствует комплексная защита информации при наличии достаточной технической защищенности
- несвоевременные сообщения или не сообщения о совершении преступлений
- низкий уровень правосознания
- уничтожение следов преступлений
- отсутствие протоколирования/оформления действий

Выводы:

Если вы ничего не видите, то это не значит, что ничего нет.

Защита информации должна быть комплексной (совокупность правовых, административных, психологических, технических и др. методов).

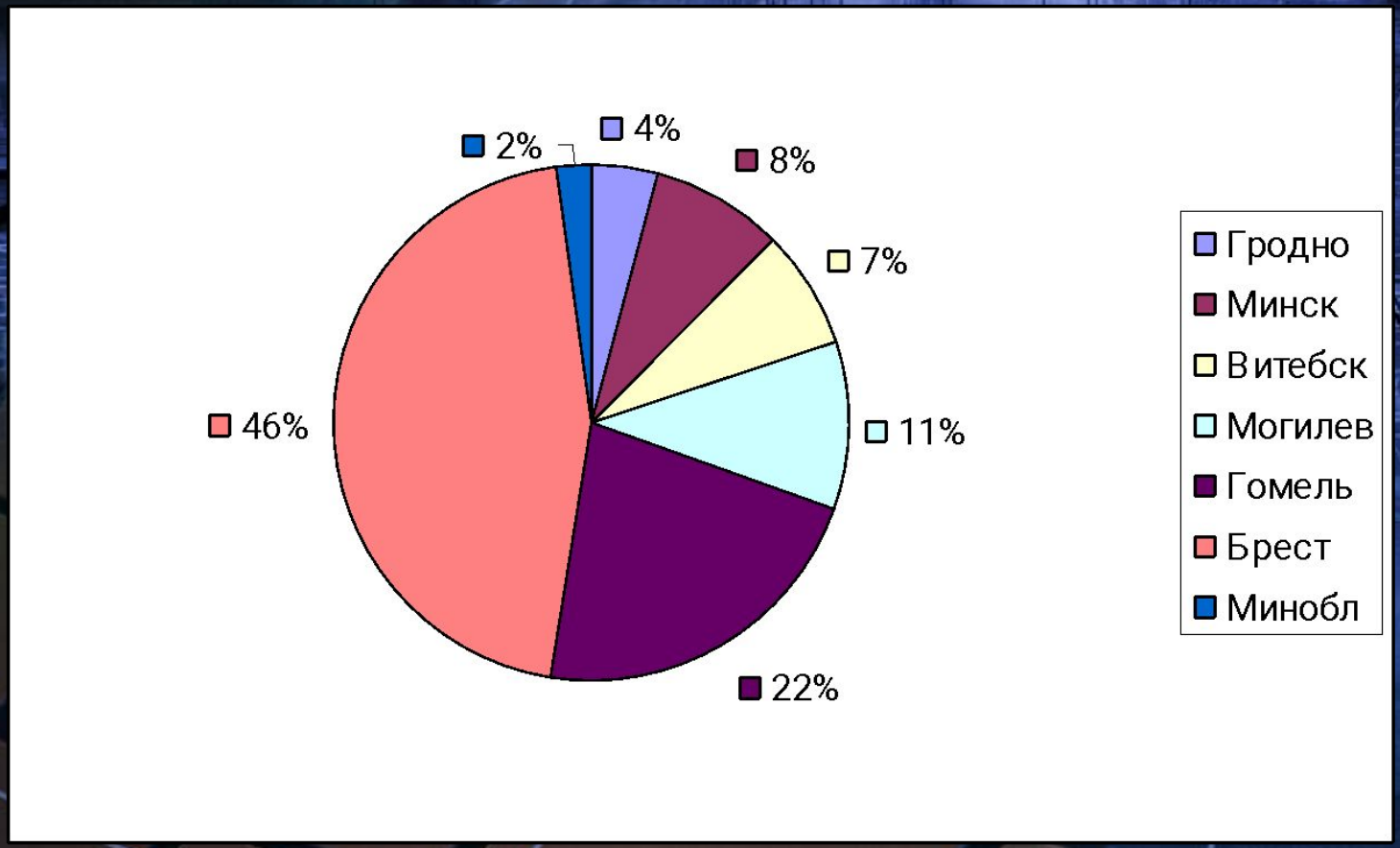
Проявления в практике:

Непосредственно «информационные» преступления

Преступления – помощники

Технологии – помощники

ст. 349 УК Республики Беларусь. Несанкционированный доступ к компьютерной информации

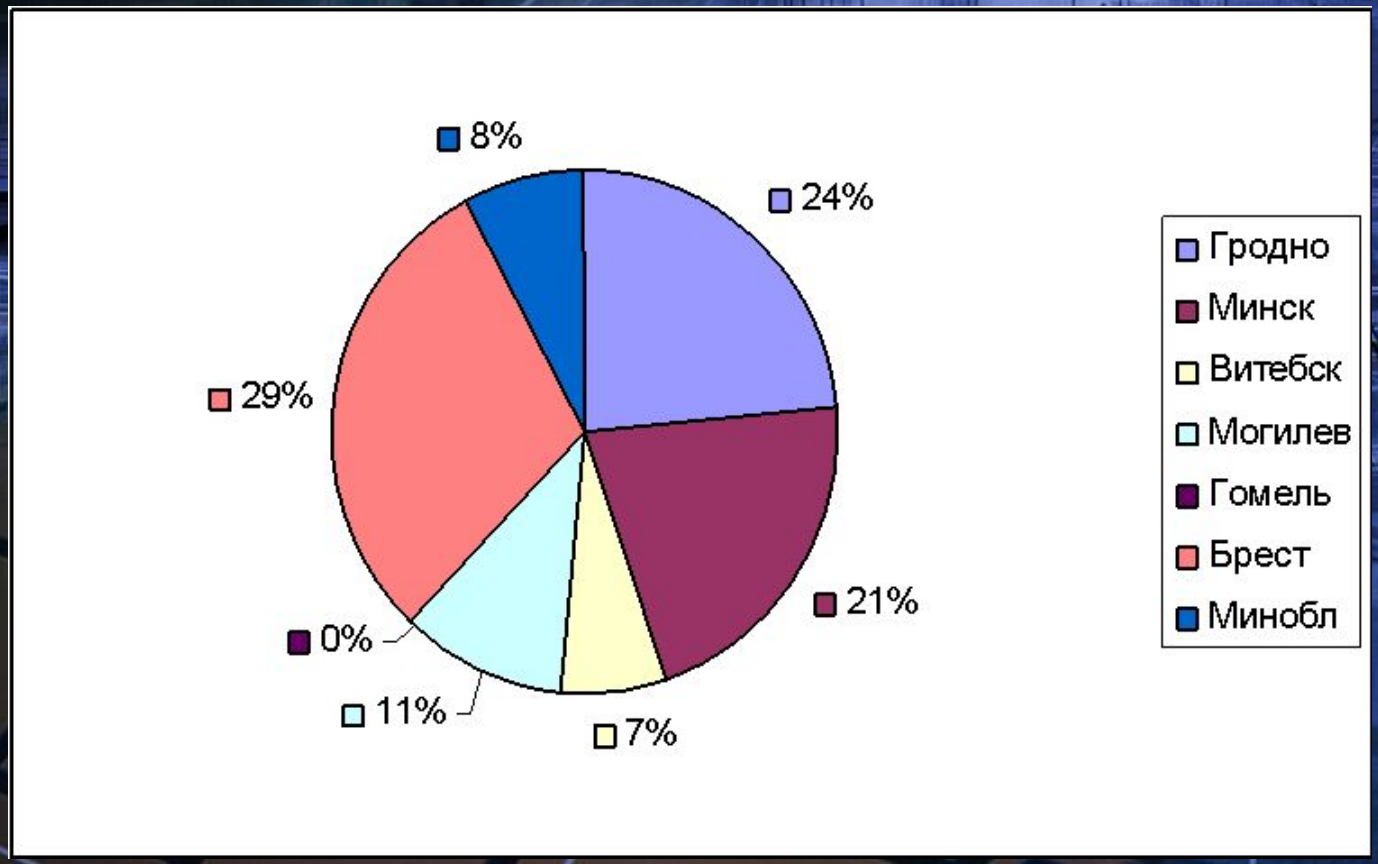


Формы совершения:

- доступ (как правило, к компьютерным сетям предприятий) в целях получения дополнительных технических возможностей

- доступ в целях получения информации или манипуляции с ней (как правило, цель доступа - обеспечение совершения других преступлений)

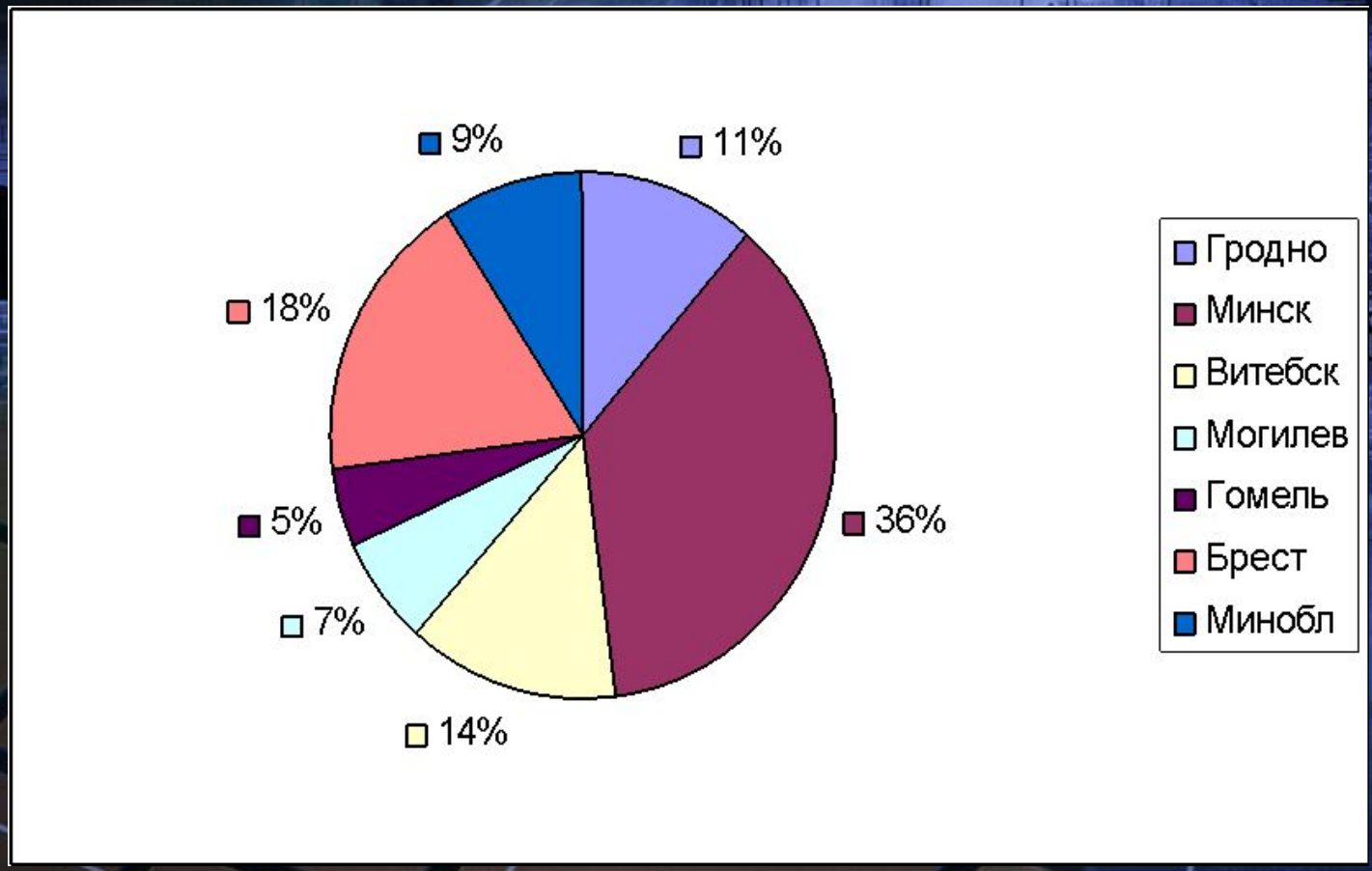
ст. 350 УК Республики Беларусь. Модификация компьютерной информации



Формы совершения:

- изменение информации (внесение заведомо ложной информации) в целях сокрытия совершенного преступления
- изменение информации в целях причинения вреда ее владельцу (как правило, путем доступа к удаленным ресурсам из хулиганских побуждений либо из-за имеющихся неприязненных отношений, а также в целях обеспечения совершения другого преступления)

ст. 351 УК Республики Беларусь. Компьютерный саботаж

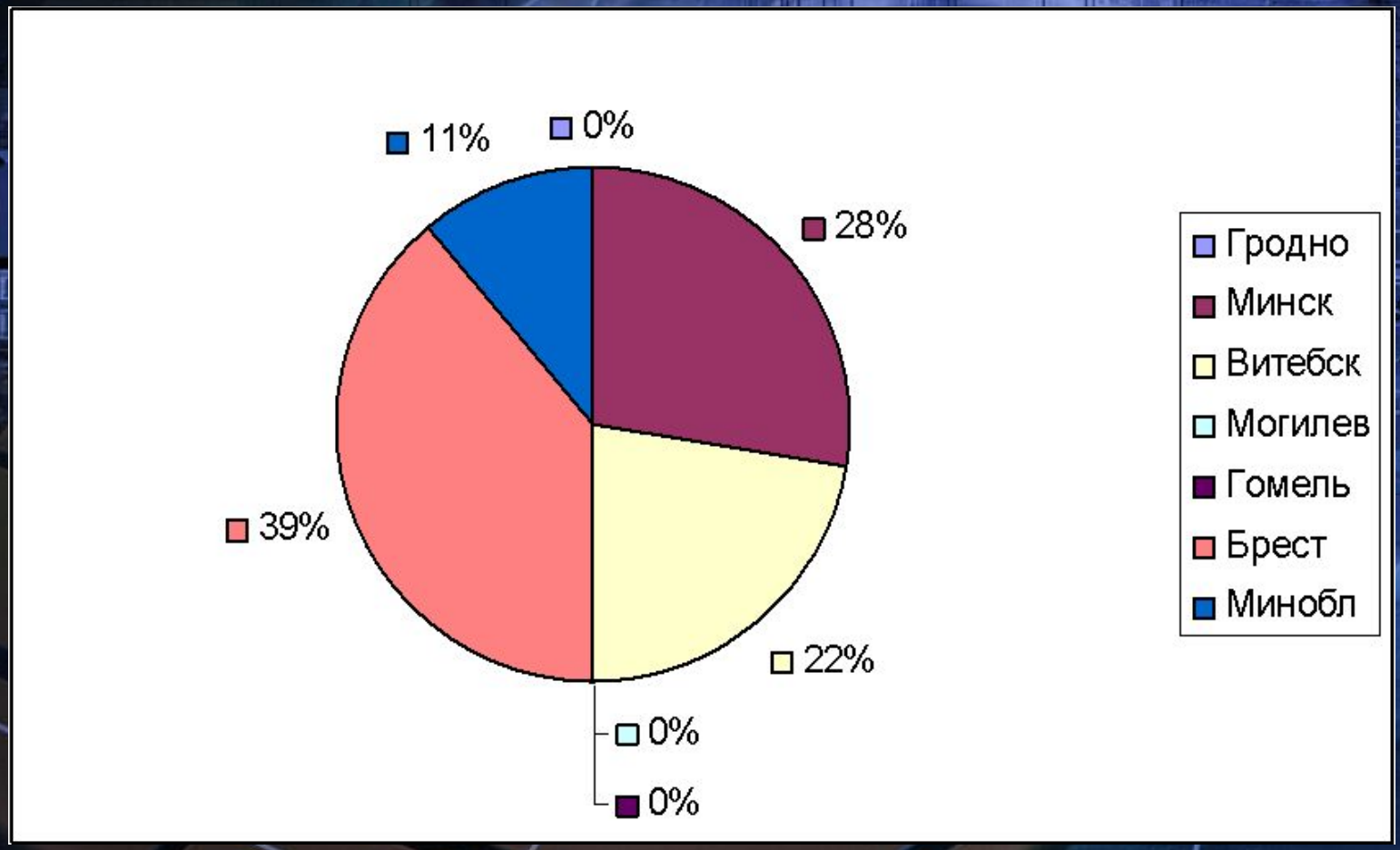


Формы совершения:

- уничтожение компьютерной информации в различных целях (из-за неприязненных отношений, чувства мести, из хулиганских побуждений, в целях показать свою значимость)

- блокирование компьютерной информации (совершается, как правило, в целях облегчения совершения другого преступления)

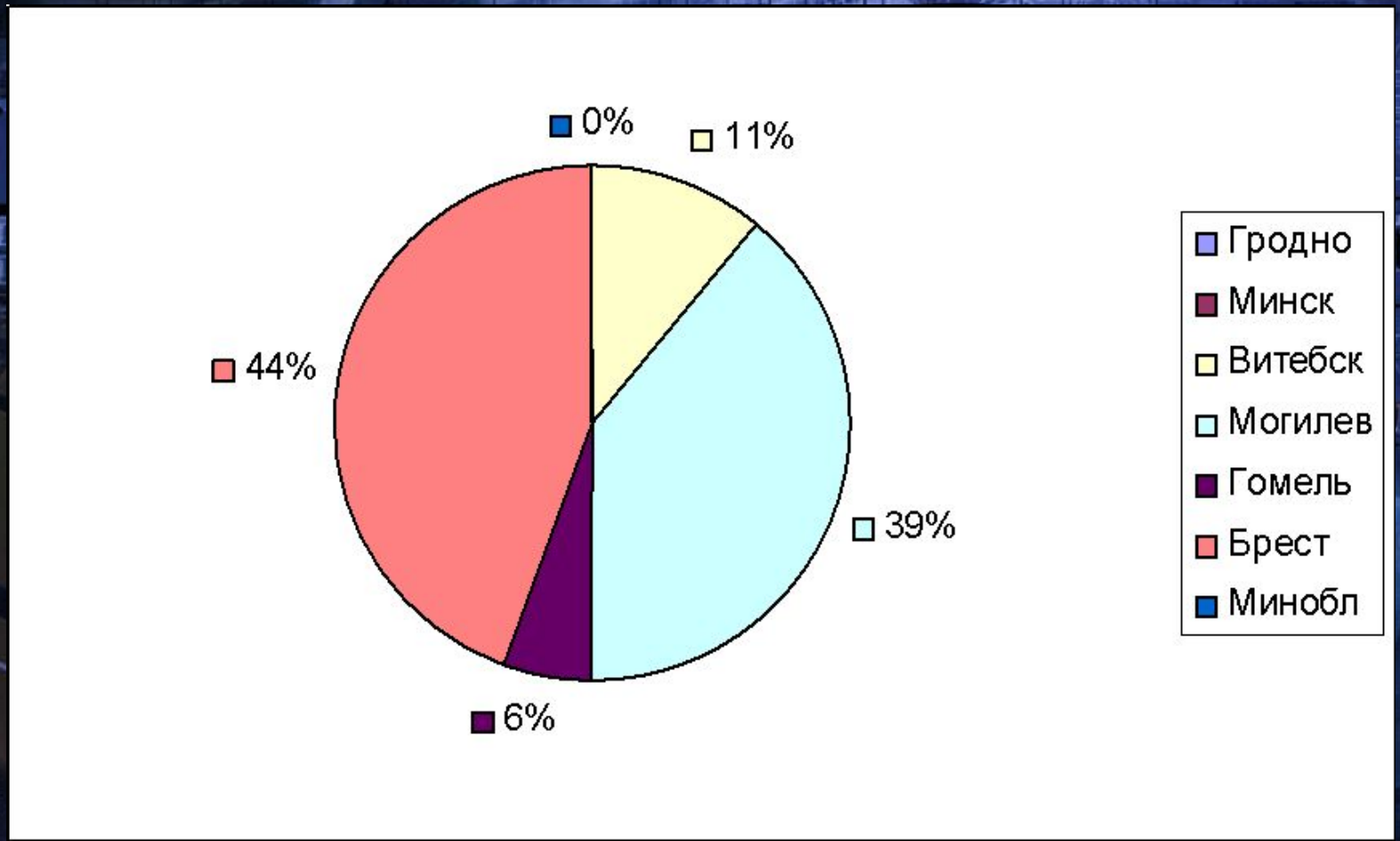
ст. 352 УК Республики Беларусь. Неправомерное завладение компьютерной информацией



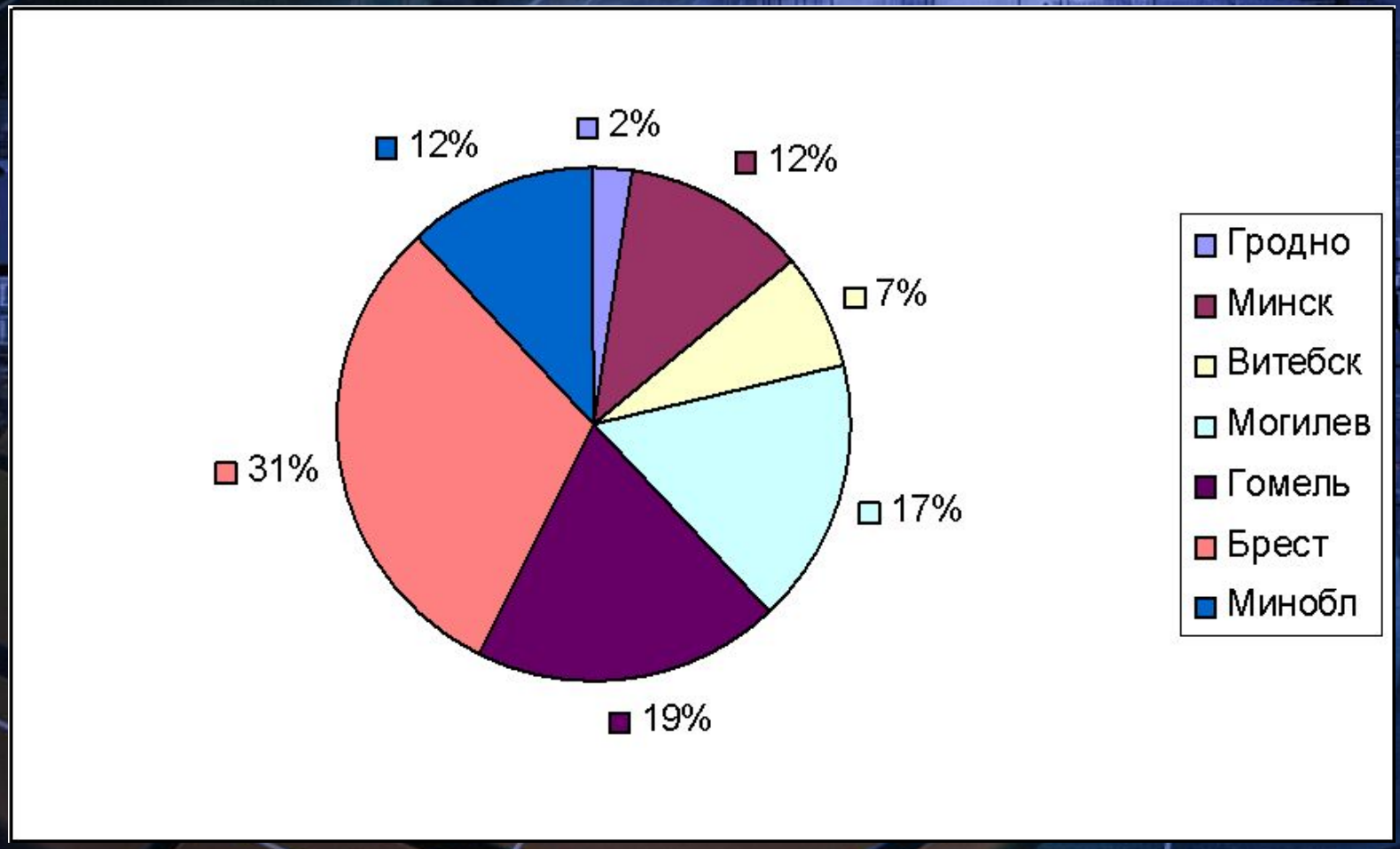
Формы совершения:

- завладение компьютерной информацией производилось лицами, как правило, не имеющими доступа к ней и находящимися от нее удаленно. Копируемая информация по содержанию представляла собой либо информацию личного характера потерпевшего (личная переписка, личные записи, фотографии, разработки), либо реквизиты доступа к другим удаленным ресурсам (например, к электронным счетам)

ст. 353 УК Республики Беларусь. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети



ст. 354 УК Республики Беларусь. Разработка, использование либо распространение вредоносных программ



Формы совершения:

- сбыт в торговых точках специальных программных средств, записанных, как правило, на лазерные диски

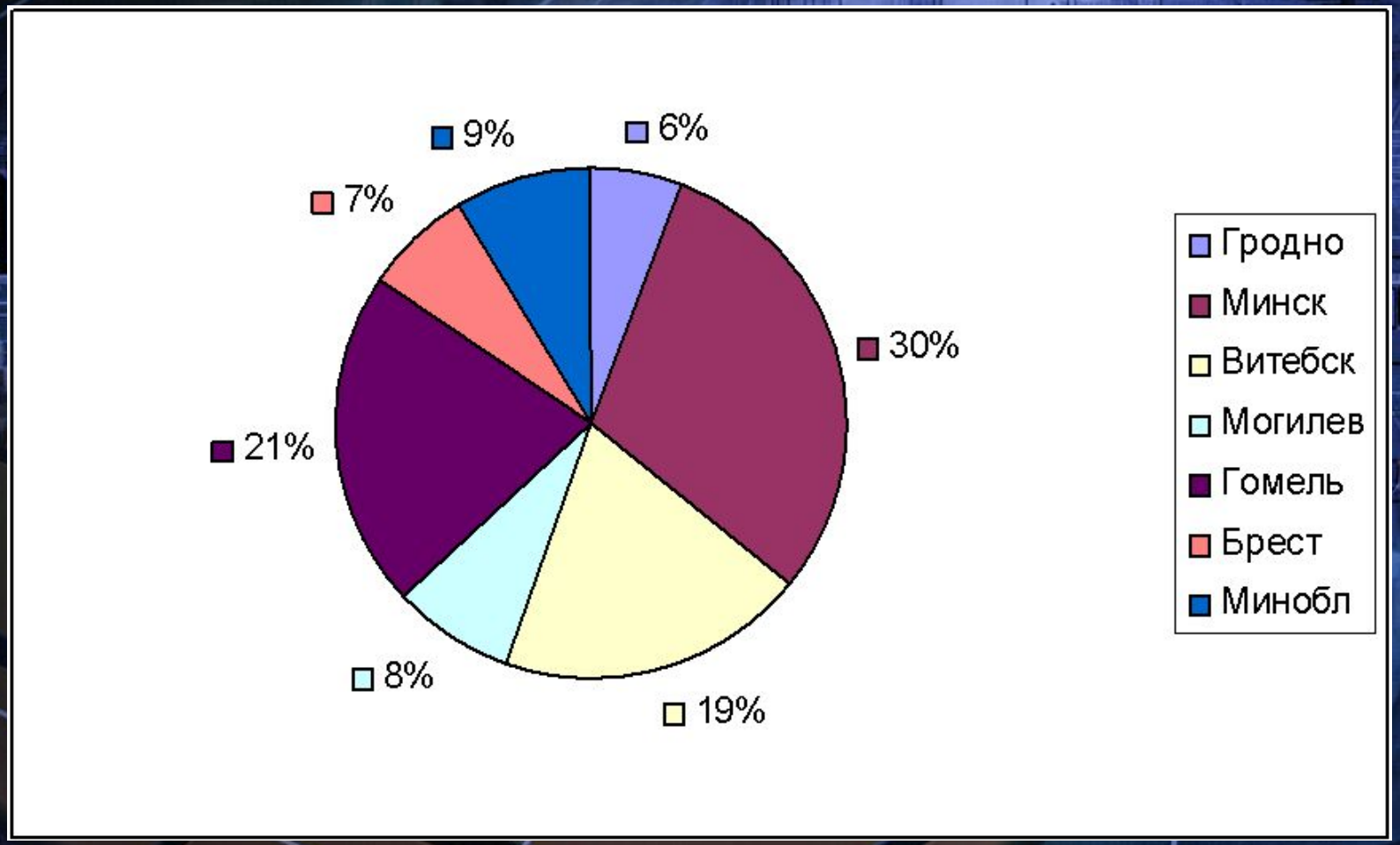
- изготовление специальных программных средств для непосредственного использования или сбыта

ст. 355 УК Республики Беларусь. Нарушение правил эксплуатации компьютерной системы или сети

Уголовные дела по ст. 355 не расследовались. Решения о возбуждении уголовных дел не принимались из-за неоднозначного толкования термина «правила».

Под «правилами» понимались лишь нормы, официально закрепленные в нормативных правовых актах. Правила, устанавливаемые субъектами, предоставляющими другим лицам компьютерные ресурсы, при этом не учитывались.

ст. 212 УК Республики Беларусь. Хищени
путем использования компьютерной техники



Формы совершения:

- «кардинг» - «вещевой», «реальный пластик», «белый пластик», «обнал» (использование реквизитов банковских пластиковых карточек лицами, не являющимися их держателями)
- хищения электронных денег
- хищения, совершаемые лицами, работающими с компьютерной информацией, которая использовалась для совершения хищений

История

Повод

Компетентная информация:

«Случаи подделки микропроцессорных карточек … в мире не зафиксированы.»

Результат:

«Неустановленное лицо в период с 11:41 по 13:53 23.03.2006 путем изменения информации, хранящейся на машинном носителе - микроконтроллере с областью памяти типа EEPROM, составляющем банковскую пластиковую карточку … и последующего введения в компьютерную систему банкоматов …, расположенных в г. Минске по адресам: …, ложной информации о правомерном использовании банковской пластиковой карточки и о наличии в распоряжении денежных средств, совершило хищение наличных денежных средств в особо крупном размере на общую сумму 45 800 000 рублей Национального Банка Республики Беларусь …» (из материалов уголовного дела)

Механизм преступления:

- специалист подразделения информатики и автоматизации банка
- дома установил банковские программы, устройство чтения карточек
- разработал и использовал специальную программу анализа данных, передающихся от устройства при использовании карточки
- модифицировал личную карточку, используя сведения карточки, подлежащей уничтожению
- совершил хищение

Благодарю за внимание!

Заместитель начальника управления по расследованию преступлений в сфере высоких технологий и против интеллектуальной собственности ГУПР МВД Республики Беларусь
Александр Макаревич

Контактный телефон: +37517-2187705
E-mail: makch@bsu.by