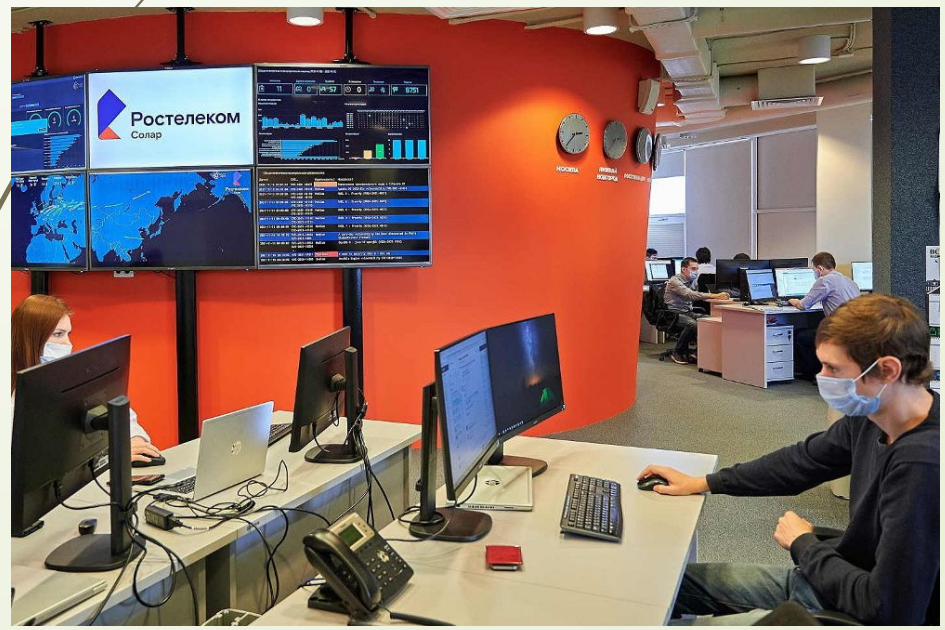
МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный университет экономики и управления «НИНХ»
(ФГБОУ ВО «НГУЭУ», НГУЭУ)

Обеспечение безопасности сайтов. Цель и сущность, объекты охраны, методы и средства.

Выполнил: студент группы сПО802,
Григорьев Владимир

Цель обеспечения безопасности сайтов

Разработчики не всегда уделяют особое внимание полной защите и безопасности созданных сайтов, хотя она и играет очень важную роль, потому что каждый сайт так или иначе может быть подвергнут взлому хакеров, если учитывать то, что сайты могут быть, самые что ни на есть, разнообразные: электронные библиотеки, социальные сети, Web-порталы различных учебных заведений, онлайн-магазины, официальные сайты всяких организаций, банков и прочее.



В Ростове-на-Дону открылся филиал крупнейшего в России коммерческого центра противодействия кибератакам, который обеспечит киберзащиту организаций Южного и Северо-Кавказского федеральных округов (ЮФО и СКФО), а также ряда крупных федеральных заказчиков.

Даже во время появления первых Web-сайтов взломщики осуществляли атаки на сайты немаловажных организаций, например, такой как, американский СитиБанк (1994г.), в результате чего было украдено 12 млн. долларов, жертвой так же стали и сайты НАТО, ЦРУ, и Минюста США.

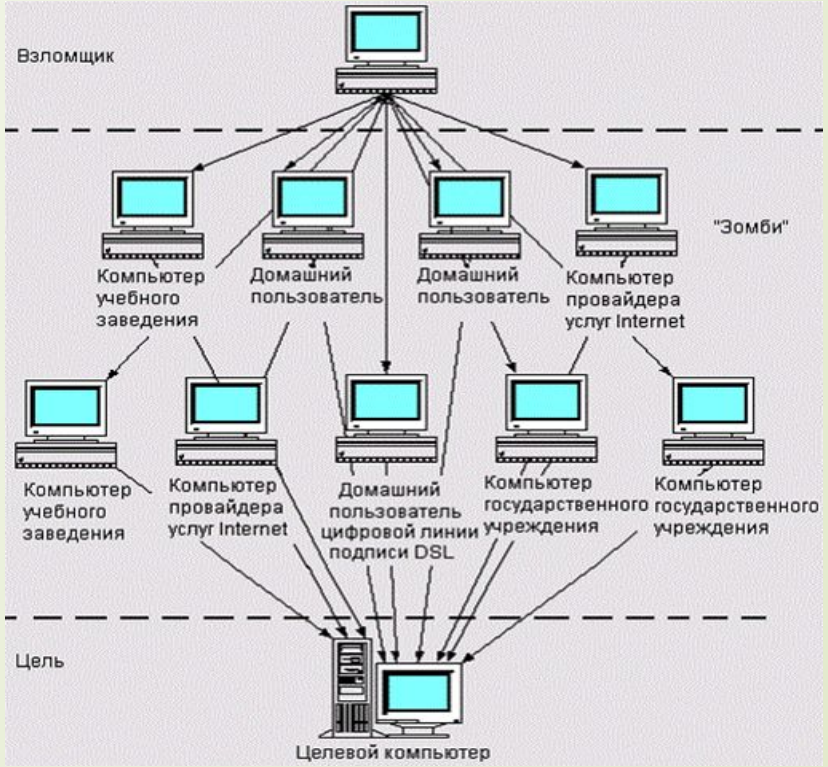
Наиболее распространенные действия правонарушителей кибератак над взломанными сайтами, которые зачастую применяются и по сей день:

- получили несанкционированный доступ к серверу, где были собраны очень стоящие сведения;
- атаковали базу данных о владельцах пластиковых карт банка; украли данные, касающиеся номеров счета основных держателей банковской карты, их имен, фамилий, контактной информации, а затем похитили крупное количество денег;
- создали вирусы, которые легко взламывали пароли, а после использовали зараженные машины для рассылки спама или как базы для хранения украденной информации;
- предприняли атаки на интернет-сайты официальных (правительственных) учреждений различных стран;
- Dos-атаки (Denial of Service — “отказ в обслуживании”) на сеть с целью переполнения ее дополнительными запросами так, чтобы полезный трафик либо снижался до минимума, либо вовсе прерывался;

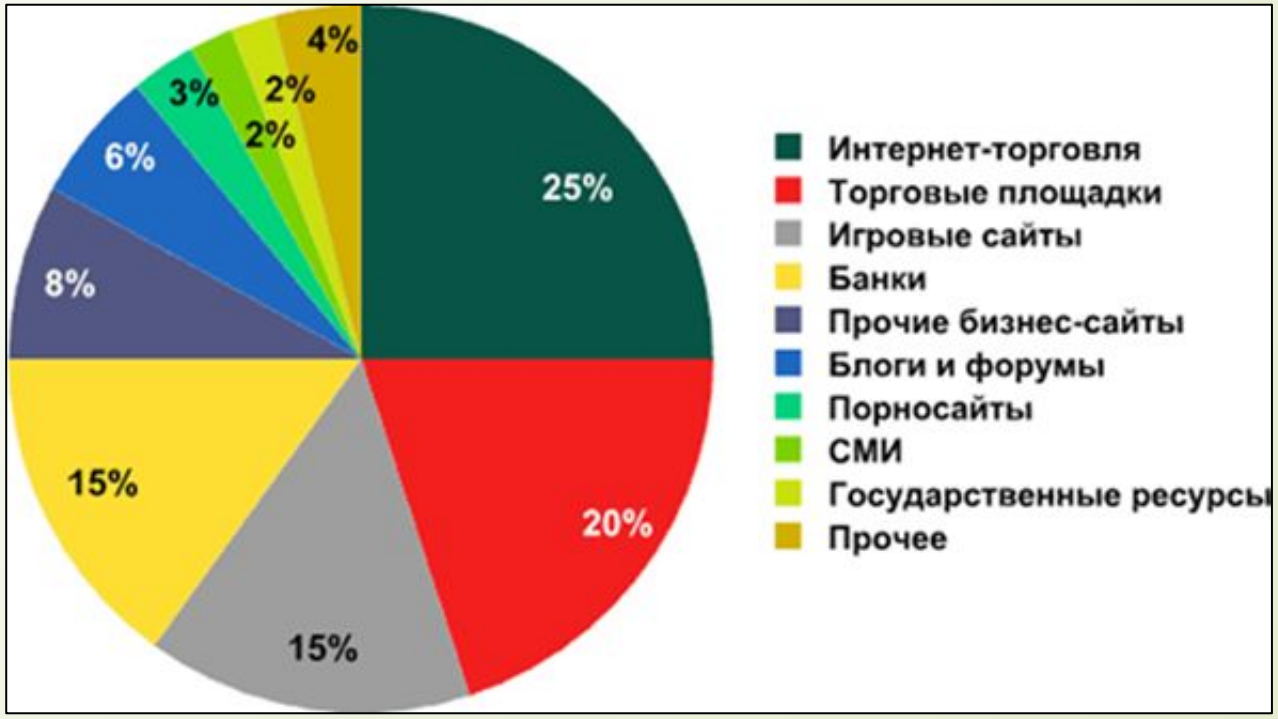
Лаборатории по предотвращению различных вирусов больше всего стали уделять внимание разработке средств противодействия DDoS атакам

DDoS атака — это действия злоумышленников, направленные на нарушение работоспособности инфраструктуры компании и клиентских сервисов атакуемому сайту. Для этого в атакуемую систему направляется огромное количество запросов, с которыми та справиться не может. Обычно для этой цели используются скомпрометированные системы.

Принцип осуществления DDoS-атаки



Главными жертвами DDoS-атак в основном остаются интернет-магазины и торговые площадки



При создании нового сайта разработчики могут воспользоваться либо уже существующими платформами, а точнее CMS (система управления контентом), либо написать все с нуля, но чаще всего малые компании предпочитают пользоваться готовыми инструментами.

Основные функции CMS:

- предоставление инструментов для создания содержимого, организация совместной работы над содержимым;
- управление содержимым: хранение, контроль версий, соблюдение режима доступа, управление потоком документов и т. п.;
- публикация содержимого;
- представление информации в виде, удобном для навигации, поиска.

Самые популярные способы защиты CMS-ок от различных атак:

1.Защита от XSS-инъекций;

2.Скрытие лишней информации;

3.Принудительное использование SSL;

4.Защиты корневого файла;

5.Методы предотвращение спамеров и ботов;

6. “Уничтожение” админа;

7.Защита директорий на сервере от просмотра.

Внедрение современных средств защиты является неотъемлемой частью мероприятий по обеспечению информационной безопасности.

Существует множество средств защиты Web-сайтов, но какими бы они не были эффективными все равно необходимо периодически тестировать Web-сайты на уязвимости, которыми в любой момент может воспользоваться взломщик.

Вопросы

1. В чём состоит цель обеспечения безопасности сайтов?
2. Что понимается под термином «кибершпионаж»?

Спасибо за внимание