3. О комсомоле и молодёжи: Сборник / В. И. Ленин. М. И. Калинин. С. М. Киров. Н. К. Крупская. В. В. Куйбышев. А. В. Луначарский. Г. К. Орджоникидзе. М. В. Фрунзе. К. Е. Ворошилов. – М.: Мол.гвардия, 1970. – 447 с.
4. Ворошилов К. Е. О проекте закона о всеобщей воинской обязанности : Доклад Народного Комиссара Обороны СССР тов. К. Е. Ворошилова на внеочередной Четвёртой сессии Верховного Совета СССР 1-го созыва 31 августа 1939 г. / Ворошилов К. Е. – М.: Политгиз, 1939. – 30 с.
5. Ворошилов К. Е. Рассказы о жизни: (Воспоминания). Кн. 1 / Ворошилов Климент Ефремович. – М.: Политиздат, 1968. – 368 с.

Мир на грани военной IT-революции?

Е.В. Гнедаш, студ. гр. 17В20
Научный руководитель: Пономарёв В.А., доц. каф. ГОИЯ
Юргинский технологический институт (филиал)
Национального исследовательского Томского политехнического университета
652055, Россия, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел. 8-913-439-98-84
E-mail: sunshine9494@rambler.ru

Информационные технологии пронизывают все сферы нашей жизни, несут с собой не только огромные выгоды, но и не менее реальные вызовы и угрозы.

Уже ни для кого не секрет, что в современных условиях для защиты страны недостаточно только традиционной мощной армии. Военные во всем миром считают, что сегодня киберпространство - пятое измерения ведения войны. Наряду с сушей, морем, воздухом и космическим пространством. Истребители, корабли, танки, артиллерия и обученные спецназовцы становятся просто бесполезными против группы хакеров. Виртуальные схватки в двадцать первом веке также важны, как и воздушные сражения в двадцатом столетии. Сегодня с помощью нескольких компьютеров можно вывести из строя любую электронную подстанцию, спутник или отключить оборонные системы. Для того чтобы ввергнуть страну в хаос, необходимо лишь отключить электричество.

Кибервойны уже стали реальностью. 2010 год. Тогда весь мир узнал про новую сложнейшую и опаснейшую вредоносную программу – «червь», который способен захватывать контроль над промышленными объектами. Его назвали «Stuxnet». Он поразил сразу сорок пять тысяч компьютеров. Большинство из них принадлежали иранским военным ведомствам. В результате нападения произошла серьезная авария на подземном заводе по обогащению урана (30 км к северу от иранского города Натенз), который являлся важнейшим элементом иранской ядерной программы. 1368 центрифуг были уничтожены, а производительность уцелевших упала на 20 процентов. Так удалось отбросить ядерную программу страны на несколько лет назад.

Stuxnet - 15 000 строк высококлассного, профессионального кода. На его создание ушло не менее четырех лет коллективного труда и более 4 млн. долларов.

NewYorkTimes пролила свет на происхождение вируса Stuxnet. Издание утверждает, что это часть секретной операции OlympicGames США, начатой еще в 2006 году при Джордже Буше и ускоренной при Бараке Обаме. Операция в Натензе проводилась американцами совместно с англичанами и подразделением 8200 разведки Израиля, имевшей там агентуру.

Это первый известный компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами и рабочими станциями. Уникальность программы заключалась в том, что впервые в истории кибератак вирус физически разрушал инфраструктуру.

В этой истории до сих пор остались загадки. Для распространения Stuxnetне нужно, чтобы компьютер был подключен к Интернету. Поначалу, расследующие инциденты специалисты предположили, что червь попал к жертвам через USB-накопители, подключенные к компьютеру. Однако анализ следов самой ранней атаки показал, что первый экземпляр Stuxnet был скомпилирован за считанные часы до заражения. За такой короткий промежуток времени крайне маловероятно успеть собрать вредоносную программу, записать ее на USB-носитель и обеспечить доставку на компьютер жертвы.

«Stuxnet не крадет деньги, не шлет спам и не ворует конфиденциальную информацию, - оценивает «червя» Евгений Касперский. - «Зловред» создан, чтобы контролировать производственные

процессы и управлять огромными производственными мощностями. В недалеком прошлом мы боролись с киберпреступниками и интернет-хулиганами, теперь наступает время кибертерроризма, кибероружия и кибервойн…».

«Это первая в мире вредоносная программа, которую можно назвать кибернетическим оружием и использовать в войне. С созданием Stuxnet была открыта новая глава в истории человечества. В настоящее время мы не знаем способа, с помощью которого можно остановить или контролировать распространение этого кибероружия в мире», - отмечает Ральф Лэнгер, немецкий IT-специалист.

В настоящее время Stuxnet распространяется по миру с большой скоростью, хакеры создают упрощенные копии червя, которые проще загружать в компьютер. Созданный спецслужбами вирус выходит из-под контроля. Эксперты предупреждают правительства всех стран, что в случае войны эта программа будет использована как полноценное кибероружие, для захвата контроля над электростанциями, трубопроводами и системами управления воздушными полетами[1].

После атаки Stuxnet государства стали усиленно наращивать свой в потенциал в киберсфере – в том числе и военный. Происходит создание специализированных структур, ответственных за кибербезопасность и кибероборону. Формируются киберотделы при министерствах обороны ведущих государств. Создаются отдельные киберкомандования, разрабатываются стратегии поведения в киберпространстве и даже проводятся масштабные военные учения с имитацией кибервойны.

Также президент Барак Обама подписал документ, по которому армия США может официально нападать на компьютерные системы своих противников, чтобы выводить их из строя. Теперь для уничтожения врага не нужны дорогостоящие бомбы и годы на разработку быстрой ракеты. Эксперты считают, что это заявление американского правительства станет настоящим толчком для новой гонки вооружения, но уже в киберпространстве.

Чем ответит Россия на фантасмагорический, но, увы, донельзя реальный вызов времени?

В 2014 году появился новый род войск в составе наших Войск воздушно-космической обороны. Пока его условно называют киберкомандованием, и оно будет противодействовать угрозам в информационных сетях общего пользования. Минобороны закупило защитный набор от хакерских атак на официальный сайт ведомства и утечки информации по внутренним каналам[2].

Кибернетические атаки могут стать идеальными инструментами следующих войн – они стремительны, эффективны в своей разрушительности и, как правило, анонимны. Уже очевидно, насколько будущие войны будут отличаться от прошлых. В преимуществе точечные атаки, выводящие из строя системы управления войсками противника, захват его информационно-телекоммуникационной инфраструктуры. Так виртуальные войны обретают вполне реальные последствия.

Источники и литература.

1. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы// [Электронный ресурс] - Режим доступа:http://www.crime.vl.ru/index.php?more=1&p=3626
2. А. Савельев, П. Карасев. Кибероружие и стратегическая стабильность /Разоружение и безопасность 2013-2014: Стратегическая стабильность: проблемы безопасности в условиях перестройки международных отношений // [Электронный ресурс] - Режим доступа:http://www.imemo.ru/files/File/ru/publ/2014/2014_035.pdf

«Зверский героизм» или мужество четвероногих

Т.Ю. Зорина, студ. гр. 17В20
Научный руководитель: Пономарёв В.А., доц. каф. ГОИЯ
Юргинский технологический институт (филиал)
Национального исследовательского Томского политехнического университета
652000, Россия, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел. 8-(38451)-6-05-37

Великая Отечественная война… Один из самых страшных периодов в истории нашей страны. Однако именно в это время оказались ярко выражены такие качества как взаимопомощь, преданность, отвага, дружба, мужество. В те годы рядом с солдатами на фронте воевали и те, кого мы называем братьями нашими меньшими: птицы и звери. Они не получили орденов, им не были присвоены