Тема1. Введение в специальность

Групповое занятие №1.
Угрозы информационной безопасности и информационные войны

Учебные вопросы:

1. Угрозы информационной безопасности и их классификация.

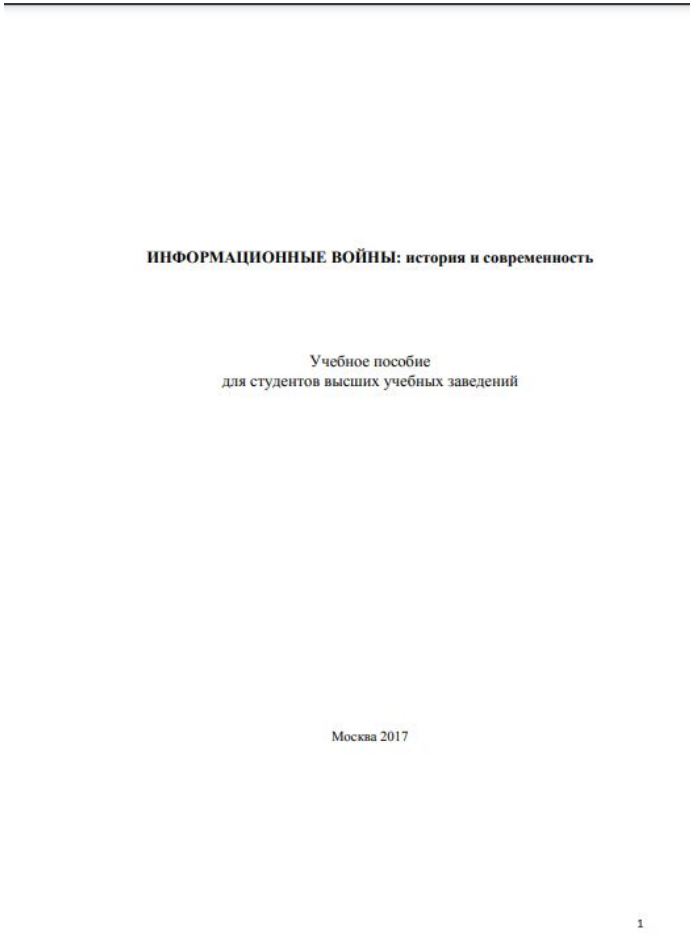
2. Общие сведения об информационных войнах.

Литература

1. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ФОРУМ : ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189337 (дата обращения: 03.02.2022). – Режим доступа: по подписке., с. 43-54.

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 03.02.2022). – Режим доступа: по подписке., с. 6-12.

Литература


ИНФОРМАЦИОННЫЕ ВОЙНЫ: история и современность

Учебное пособие
для студентов высших учебных заведений

Москва 2017

1

3. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. – 124 с. .: ил. https://mgimo.ru/upload/iblock/486/Сулейманова%20Ш.С.%20Назарова%20Е.А.%20-%20ИНФОРМАЦИОННЫЕ%20ВОЙНЫ.pdf (дата обращения: 03.02.2022). – Режим доступа: свободный., С. 46-57, 81-85.

Одна из реальных и относительно новых глобальных угроз безопасности компьютерных систем - это **информационное оружие**

Даже незначительные случайные нарушения нормального функционирования компьютеров могут нанести существенный урон особо уязвимым системам управления и планирования

Действительно серьезной проблемой становятся не случайные сбои компьютеров, а опасность специального и целенаправленного воздействия на информационные ресурсы противником

Информационное пространство фактически стало театром военных действий, где каждая противоборствующая сторона стремится получить преимущество, а при необходимости - разгромить противника.

Размах противоборства в информационной сфере достиг таких масштабов, что потребовалось создание специальной концепции получившей название информационной войны или информационного противоборства.

Вопрос №1. Угрозы информационной безопасности и их классификация

Под ***угрозой информационной безопасности*** **Российской Федерации** (далее - **информационная угроза**) понимается - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Угроза- это потенциальная возможность определенным образом нарушить информационную безопасность

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

Угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое *место*, и до момента, когда *пробел* ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом. Пока существует *окно опасности*, возможны успешные атаки на ИС.

Замечание 1.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении «заплат», ее исправляющих.

Замечание 2.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

- *должно стать известно о средствах использования пробела в защите;*
- *должны быть выпущены соответствующие «заплаты»;*
- *заплаты должны быть установлены в защищаемой ИС.*

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность);
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Наиболее распространенные угрозы ДОСТУПНОСТИ

Самыми частыми и самыми опасными (с точки зрения *размера ущерба*) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Основной способ борьбы с непреднамеренными ошибками - автоматизация и административный контроль.

Другие угрозы доступности классифицируются по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой;
- невозможность работать с системой в силу отсутствия соответствующей подготовки;
- невозможность работать с системой в силу отсутствия технической поддержки.

Основными источниками *внутренних отказов* являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала;
- ошибки при (пере) конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рассматривают следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т. п.).

ВЫВОД:

Несмотря на предпринимаемые дорогостоящие меры функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации.

Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, ***что такое угроза безопасности*** информации, выявить ***возможные каналы утечки*** информации и ***пути несанкционированного доступа*** к защищаемым данным.

Вопрос №2.
Общие сведения об информационных войнах

Любое государство должно признавать наличие угрозы информационных боевых действий и постоянно заботиться о защите национальных информационных ресурсов и сохранении конфиденциальности информационного обмена через сети обмена информацией

Следует отличать информационную войну от компьютерной преступности.

Любое компьютерное преступление представляет собой факт нарушения того или иного закона.

Компьютерное преступление

случайным

специально спланированным

обособленным

составной частью обширного плана атаки

Ведение **информационной войны** в отличии от компьютерных преступлений никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий.

Театр боевых информационных действий простирается на такие сферы как:

- электронное поле боя
- атаки сетей обмена информацией автоматизированных систем управления
- атаки сетей обмена информацией инфраструктуры
- промышленный шпионаж
- конфиденциальность
- другие виды разведки

Информационная война (ИВ) – использование и управление информацией с целью получения конкурентного превосходства над противником

ИВ может включать сбор тактической информации, обеспечение безопасности собственных информационных ресурсов, распространение пропаганды или дезинформации, чтобы деморализовать противника и население, подрыв качества информации противника и предупреждение возможности сбора информации противником.

В последнее время часто ИВ ведется в комплексе с **кибер-** и **психологической войной** с целью более широкого охвата целей, с привлечением радиоэлектронной борьбы и сетевых технологий.

Кибервойна (англ. Cyberwarfare) — противоборство (война) и противостояние в кибернетическом пространстве (киберпространстве), в том числе компьютерное противостояние в Интернете, одна из разновидностей информационной войны.

Психологическая война (син. психологические операции) — психологическое воздействие на войска (силы) противника и население с целью их деморализации и склонения к прекращению сопротивления.

Цель информационной войны – ослабить моральные и материальные силы противника или конкурента и усилить собственные.

Главная задача ИВ заключается в манипулировании массами

Цель такой манипуляции зачастую заключается в следующем:

- внесение в общественное и индивидуальное сознание враждебных, вредных идей и взглядов;
- дезориентация и дезинформирование масс;
- ослабление определенных убеждений и устоев;
- запугивание своего народа образом врага;
- запугивание противника своим могуществом.

Виды информационных войн:

- психологическая война
- кибервойна
- сетевая война
- идеологическая диверсия
- радиоэлектронная борьба

Радиоэлектронная борьба (**РЭБ**) — разновидность вооружённой борьбы, в ходе которой осуществляется воздействие радиоизлучениями (радиопомехами) на радиоэлектронные средства систем управления, связи и разведки противника в целях изменения качества циркулирующей в них военной информации, защита своих систем от аналогичных воздействий, а также изменение условий (свойств среды) распространения радиоволн.

Сетевая война (Netwar) – это конфликт социетального (общества в целом) уровня, проходящий с помощью интернет коммуникаций.

Идеологическая диверсия (англ ideological diversion) - заведомо ложная, дезориентирующая политическая или иная информация, пропаганда не соответствующих действительности утверждений, фактов, теорий и т. п. в целях дестабилизации политической ситуации в государстве.

Основным средством ведения ИВ является информационное оружие (ИО)

К ИО относятся следующие средства:

- уничтожения, искажения или хищения информационных массивов;
- преодоления систем защиты;
- ограничение допуска законных пользователей;
- дезорганизация работы технических средств, компьютерных систем.

Атакующим информационным оружием сегодня можно назвать:

- компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п.;
- логические бомбы – программные закладные устройства, которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу в установленное время привести их в действие;
- средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного, военного, экономического и общественного управления;
- средства нейтрализации тестовых программ;
- различного рода ошибки, сознательно вводимые лазутчиками в программное обеспечение объекта

Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем.

Объектом внимания при ведении информационной войны становятся:

- информационные системы
- сети обмена информацией
- информационные технологии, используемые в системах вооружений

Так как **информационная война**, имеющая целью изменить расстановку сил в мире, связана с вопросами информации и коммуникаций, то, если смотреть в корень, это есть **война за знания** - за то, кому известны ответы на вопросы: что, когда, где, почему и насколько надежным считает отдельно взятая страна и ее армия свои знания о себе и своих противниках.

Если **наступательная** составляющая информационной войны связана с разработкой и использованием информационного оружия, то основными аспектами **оборонительной** составляющей являются, обнаружение, реагирование и защита.

Таким образом, развитие и совершенствование компьютерных и информационных технологий, создает предпосылки к разработке и применению информационного оружия.

Заключение

Владение эффективным информационным оружием и средствами защиты от него становится одним из главных условий обеспечения национальной безопасности государства в XXI веке.