МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению практических работ
по дисциплине «Информационная безопасность в электроэнергетике»
для студентов направления подготовки
13.03.02 Электроэнергетика и электротехника

Содержание

ния дисциплины

5.2 Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

5.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Цель и задачи изучения дисциплины

Целью освоения дисциплины «Информационная безопасность в электроэнергетике» является изучение основных принципов обеспечения защиты информации и защиты от кибернетических угроз объектов электроэнергетики, правовых, организационных, программных, технических и алгоритмических способов защиты, используемых для оценки угроз и мер защиты моделей, существующей законодательной базы в области защиты информации и отраслевых стандартов.

Задачи освоения дисциплины: формирование у студентов представления о видах защищаемой информации, классификации кибернетических угроз на объектах электроэнергетики, различных способах защиты, принципах их действия и методиках выбора средств защиты в соответствии с угрозами, рисками и их последствиями.

2. Оборудование и материалы

Аппаратные средства: переносной ноутбук, проектор, интерактивная доска.

Учебная аудитория для проведения учебных занятий, оснащена оборудованием и техническими средствами обучения.

3 Наименование практических работ

Для студентов заочной формы обучения предусмотрены практические работы: Практическая работа №2 Информационное противодействие. Информационные войны. Кибератаки. и Практическая работа №3 Влияние надежности цифровых подсистем на общую надежность электроэнергетических систем

Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
Роль информационной безопасности в современном обществе	2	
Информационное противодействие. Информационные войны. Кибератаки.	2	
Влияние надежности цифровых подсистем на общую надежность электроэнергетических систем	2	
Вредоносное программное обеспечение и методы борьбы	2	
Интернет угрозы и методы борьбы с ними	2	
Современные системы управления информационной безопасностью	2	
Электронно-цифровая подпись. Система удостоверяющих центров. Сертификаты.	2	
Моделирование угроз кибербезопасности	2	
Экономическая эффективность средств обеспечения информационной безопасности	2	
Итого за 4 семестр:	**18**	
Итого:	**18**	

4. Содержание практических работ

Практическая работа №1

Роль информационной безопасности в современном обществе

Цель: изучить основные положения нормативного документа «Доктрина информационной безопасности РФ» от 6 декабря 2016 г.

1. **Основы теории**

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов.

Значимость обеспечения безопасности государства в информационной сфере подчеркнута в принятой в декабре 2016 года «Доктрине информационной безопасности Российской Федерации»: "Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать".

2. Порядок выполнения работы

Задание 1. Изучить содержание «Доктрины информационной безопасности РФ» 6 декабря 2016 г., национальные и международные документы в области защиты информации, а также лекционный материал по соответствующим темам. https://www.garant.ru/products/ipo/prime/doc/71456224/

Задание *2*. Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы.

Контрольные вопросы:

1. Доктрина безопасности РФ.
2. Национальные и международные документы в области защиты информации.
3. Физическая защита информационных систем.
4. Программные средства защиты информации.
5. Этапы создания систем защиты информации.
6. Защита информации. Основные принципы обеспечения информационной безопасности.
7. Доктрина информационной безопасности РФ. ГОСТЫ РФ.
8. Информация. Виды информации, свойства и понятие информации в контексте информационной безопасности.

9. Понятие национальной безопасности, виды безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации.

Практическая работа №2

Тема: Информационное противодействие. Информационные войны. Кибератаки.

Цель: *изучить возможные пути реализации информационной войны в современном мире и уровни ведения информационной войны*

1. Основы теории

Отражение информационной войны в нормативно - законодательной базе Российской Федерации.

До некоторого времени в России не уделялось большого внимания понятию угроз информации, информационных ресурсов и информационной войны.

В декабре 1997 года Указом Президентом РФ была утверждена «Концепция Национальной Безопасности Российской Федерации». В редакции от 10 января 2000 года говорится что «Национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа».

Так же говориться, что «усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере. Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним». То же самое сказано и в Доктрине Информационной Безопасности Российской Федерации.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных

систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения “информационного оружия” против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Важнейшими задачами обеспечения информационной безопасности Российской Федерации, согласно Доктрине, являются:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Комплексное противодействие угрозам информационной войны входит в список первоочередных мероприятий по реализации государственной политики обеспечения информационной безопасности.

Главными направлениями совершенствования системы обеспечения информационной безопасности РФ определены:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;
- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;
- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

Для реализации основных положений Доктрины и обеспечения информационной безопасности России было создано Управление информационной безопасности в Совете Безопасности РФ.

Возможные пути реализации информационной войны в современном мире.

История всех локальных вооруженных конфликтов конца XX в., начиная с операции «Буря в пустыне» и заканчивая войной в Югославии, установлением конституционного порядка в Чеченской Республике, вооруженным конфликтом в Македонии и войной в Ираке, связана с действиями сил и подразделений, специально подготовленных для проведения операций информационной войны, деятельность которых с сопредельной с противником территории (без непосредственного вооруженного соприкосновения) начиналась, как правило, задолго до нанесения первых огневых ударов. При этом действия сил специальных информационно-психологических операций в основном были настолько успешны, что вооруженные силы противника нередко еще до начала активных боевых действий получали такой урон (связанный как с воздействием на сознание военнослужащих, так и с вызванной этим воздействием неправильной оценкой ситуации военно-политическим руководством и, как следствие, серией совершаемых им ошибок), который в минувших войнах мог быть нанесен только в результате нескольких тяжелых поражений и потери части территории страны.

Наблюдая с экранов телевизоров за «странной» войной в Ираке, мир увидел появление войн нового поколения информациошто-психологических, в которых собственно боевые действия играют подчиненную, сервисную роль, а план вооруженной кампании строится по правилам и в соответствии со сценарием пиар-воздействия на собственных граждан, на граждан политических союзников и оппонентов и на международное сообщество в целом. Таким образом, можно со всем основанием говорить о том, что современный вооруженный конфликт развивается в жанре репортажа и по законам этого жанра, с тем чтобы генерируемые им новости своим форматом максимально близко соответствовали формату пиар-материала, необходимого для реализации технологий информационно-психологического воздействия.

В настоящее время в мире накоплен и систематизирован значительный опыт ведения информационно-психологической войны (ИПВ), проведения информационно-психологических операций, разработан и опробован на практике широкий спектр средств и методов оказания информационного (информационно-психологического) воздействия. Практически все стороны, осуществляющие информационно-психологическое воздействие в своих интересах, формируют стратегию и тактику психологической войны, конкретное содержание информационно-психологических операций в соответствии со своими интересами, целями, задачами и имеющимися возможностями.

Становится реальностью и выдвигается на первый план новая группа угроз безопасности, возникающих при подготовке и ведении иностранными государствами информационной войны, в частности в регионах, являющихся традиционно сферой национальных интересов России, а также и на ее собственной территории. Одним из направлений осуществления мероприятий по подготовке и проведению информационных войн является проведение информационно-психологических операций, ориентированных на формирование условий для принятия выгодных для зарубежных государств и их деловых кругов решений в военной, политической, экономической и других областях, в странах-мишенях, являющихся объектами информационно-психологического воздействия".

В настоящее время ведущие страны мира находятся в состоянии переходного периода от индустриального этапа своего развития к индустриально-информационному, на котором главным стратегическим национальным ресурсом становятся информация, сетевая инфраструктура и информационные технологии. Завершение этого перехода ожидается во втором десятилетии XXI в., но уже сегодня информационная зависимость всех сфер жизнедеятельности личности, общества и государства чрезвычайно велика. Так, нарушение работы компьютерных и иных телекоммуникационных сетей, используемых в системах управления государственными и банковскими структурами США, путем вывода из строя вычислительных средств и средств связи или уничтожения хранящейся в сетях информации способно нанести экономике страны, занимающей лидирующие позиции в сфере информационных технологий, настолько серьезный ущерб, что его можно сравнивать с ущербом от военного вторжения.

В сложившейся обстановке ряд развитых западных государств, и в первую очередь США, в начале 90-х годов вплотную приступили к изучению и проработке проблем, связанных с противоборством в информационной сфере, или так называемой «информационной войной» (ИВ). По утверждению американских специалистов, отдельные положения концепции «информационная война» уже в течение длительного времени реализуются США на политическом уровне в основном в форме психологической войны, которая внесла свой вклад в развал СССР и Организации Варшавского Договора.

В США под этим термином понимается комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее политическое и военное руководство, которое уже в мирное время приводило бы к принятию благоприятных для Соединенных Штатов решений, а в ходе войны полностью парализовало структуру управления противника. Одновременно с наступательным воздействием информационное противоборство предполагает обеспечение надежной защиты национальной информационной инфраструктуры США.

В военном ведомстве США разработана концепция развития сухопутных сил до 2010 г. (Army Vision-2010), согласно которой основным смыслом

боевой деятельности войск становится достижение информационного превосходства. По мнению американских экспертов, завоевание или достижение информационного превосходства позволяет собирать, обрабатывать и передавать непрерывный поток информации, одновременно лишив противника способности делать то же самое. По концепции Army Vision-2010, для достижения информационного господства проводятся информационные операции.[5]

Уровни ведения информационной войны. Информационные операции. Психологические операции. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.

В настоящее время разработанная Пентагоном концепция ведения информационной войны реализуется на двух уровнях: государственном и военном.

На государственном уровне цель информационного противоборства в широком смысле слова заключается в ослаблении позиций конкурирующих государств, подрыве их национально-государственных устоев, нарушении системы государственного управления за счет информационного воздействия на политическую, дипломатическую, экономическую и социальную сферы жизни общества, проведения психологических операций, подрывных и иных деморализующих пропагандистских акций.

Информационные операции (ИО) на данном уровне могут решать задачи защиты национальных интересов США, предупреждения международных конфликтов, пресечения провокационных и террористических акций, а также обеспечения безопасности национальных информационных ресурсов.

На военном уровне информационные операции представляют собой комплекс мероприятий, проводимых в масштабах вооруженных сил страны, их видов, объединенных командований в зонах, и являются составной частью военных кампаний (операций). Они направлены на достижение информационного превосходства над противником (в первую очередь в управлении войсками) и защиту своих систем управления. Для этого могут использоваться любые военные и технические силы и средства, имеющиеся в распоряжении, при формальном соблюдении правовых, моральных, дипломатических, политических и военных норм. Перед ВС впервые поставлена задача воздействия на противника еще в угрожаемый период (до начала активных боевых действий) с тем, чтобы обеспечить выгодную для США направленность процессов управления и принятия решений противостоящей стороной.

Такое распределение задач, по оценке американских экспертов, должно обеспечить необходимую эффективность проведения мероприятий в рамках информационного противоборства, которое в теории и практике военного строительства в Соединенных Штатах стало рассматриваться в качестве особой формы межгосударственных отношений после анализа итогов войны в зоне Персидского залива.

Военное руководство США считает, что эффективное информационное противоборство должно обеспечить командирам (командующим) возможность навязать противостоящей стороне ложное видение обстановки, принудить ее к ведению военных действий в невыгодных для нее условиях. Это достигается в основном благодаря проведению комплекса мероприятий, позволяющих, с одной стороны, нарушить процесс принятия решений противником, а с другой - обрабатывать информацию по циклу принятия решений в своей системе управления эффективнее и быстрее, чем это может сделать командующий противостоящей группировкой войск.

Информационные операции

Практическая реализация концепции информационного противоборства осуществляется путем проведения информационных операций, которые представляют собой комплекс мероприятий, имеющих целью оказать воздействие на информацию и информационно-управляющие системы (ИУС) противника при одновременной защите своей информации и информационных систем. Они являются важным фактором в достижении и удержании информационного превосходства в ходе операций объединенных группировок ВС. Информационная война представляет собой соответствующую операцию, проводимую в период кризисной ситуации или конфликта (включая войну) для достижения специфических целей над специфическим противником или противниками. Применительно к информационным операциям термин «противник» рассматривается в более широком смысле. Под ним подразумеваются организации, группы лиц или отдельные лица, принимающие решения либо осуществляющие действия, направленные на срыв выполнения задач, поставленных перед командованием объединенных вооруженных сил.

Подготовка и проведение информационных операций связаны с согласованием и разрешением на уровне национального военно-политического руководства страны комплекса вопросов законодательного и политического характера. ИО проводятся на всех уровнях военных действий, границы между которыми зачастую носят условный характер.

На стратегическом уровне такие операции проводятся по решению военно-политического руководства страны и призваны обеспечить достижение национальных стратегических целей. В ходе их осуществляется воздействие на все элементы государственного устройства потенциальных противников (политические, военные, экономические и информационные) при одновременной защите своих государственных структур. Для достижения целей ИО на этом уровне должна обеспечиваться высокая степень координации между военными органами и правительственными учреждениями и ведомствами США, а также союзниками и партнерами по коалиции.

На оперативном уровне ИО проводятся для обеспечения успешного хода операции или кампании в целом или решения главных задач операции. Их цель - воздействие на линии связи, системы тылового обеспечения и боевого управления вооруженными силами противника при одновременной за-

щите аналогичных систем, как своих ВС, так и союзников. Информационные операции, проводимые на этом уровне, могут способствовать достижению стратегических целей.

Информационные операции на тактическом уровне проводятся с целью обеспечения решения тактических задач. Они сосредоточены на воздействии на информацию и информационные системы, такие, как системы связи, боевого управления, разведки и другие, непосредственно обеспечивающие ведение боевых действий соединениями и частями противника при одновременной защите как систем своих, так и союзников.

В основу концепции информационного противоборства заложена обоюдная зависимость (уязвимость) США и их потенциальных противников от информации и информационных систем. В связи с этим при ее реализации рассматриваются два аспекта деятельности — воздействие на информационную инфраструктуру противника и защита своей собственной информационной среды. Соответственно все информационные операции подразделяются на наступательные и оборонительные.

Наступательные информационные операции представляют собой комплексное проведение по единому замыслу и плану мероприятий по оперативной маскировке, радиоэлектронной борьбе, программно-математическому воздействию на ИУС, физическому уничтожению (выводу из строя) объектов информационной инфраструктуры, а также психологических и специальных ИО. В ходе таких операций принимаются меры, оказывающие воздействие на сознание людей и направленные на срыв процесса принятия решений, а также действия с целью нарушения работы или уничтожения элементов информационной инфраструктуры. Новым элементом наступательных информационных операций в сравнении с концепцией борьбы с системами управления являются специальные ИО и мероприятия по программно-математическому воздействию на компьютерные сети противника.

Оборонительные информационные операции представляют собой взаимосвязанные процессы по защите информационной среды, вскрытию признаков нападения, восстановлению боеспособности и организации ответных действий на агрессию (нападение). Их основными элементами являются: обеспечение физической безопасности информационной инфраструктуры, безопасности информации и скрытности действий войск (сил); вскрытие мероприятий по оперативной маскировке противника; контрпропаганда; контрразведка; радиоэлектронная защита и специальные информационные операции.

Оборонительные информационные операции должны обеспечивать своевременность и точность передачи данных, гарантированный доступ к ним пользователей в условиях информационного воздействия противника. В ходе их предусматривается проведение мероприятий по восстановлению боеспособности информационных систем.

Наступательные и оборонительные информационные операции могут проводиться по единому замыслу и плану и взаимно дополнять друг друга. Они ориентированы на одни и те же объекты воздействия, в качестве которых могут выступать:

- органы управления государства и его вооруженных сил;
- ИУС гражданской инфраструктуры (телекоммуникационные, включая средства массовой информации, транспортные, энергетического комплекса, финансового и промышленного секторов);
- управляющие элементы военной инфраструктуры (системы связи, разведки, боевого управления, тылового обеспечения, управления оружием);
- линии, каналы связи и передачи данных;
- информация, циркулирующая или хранящаяся в системах управления;
- общество в целом (как гражданское население, так и личный состав вооруженных сил), его государственные, экономические и социальные институты;
- руководящий состав и персонал автоматизированных систем управления, участвующий в процессе принятия решений.

Психологические операции

Психологические операции представляют собой мероприятия по распространению специально подготовленной информации с целью оказания воздействия на эмоциональное состояние, мотивацию и аргументацию действий, принимаемые решения и поведение отдельных руководителей, организаций, социальных или национальных групп и отдельных личностей иностранных государств в благоприятном для США и их союзников направлении. Они могут быть стратегическими, оперативными и тактическими по своим масштабам и их проведение может обеспечиваться мероприятиями оперативной маскировки.

На стратегическом уровне психологические операции могут проводится в форме пропаганды определенных политических или дипломатических позиций, официальных заявлений либо сообщений руководителей государства.

На оперативном уровне такие операции могут проводиться в виде распространения листовок, с помощью радио- и телевещания, вещания с использованием средств громкоговорящей связи, а также других средств для передачи информации, содержащей призывы, побуждающие личный состав вооруженных сил противника к массовому саботажу, дезертирству, бегству или капитуляции.

На тактическом уровне проведение психологических операций предполагает использование громкоговорящей связи и других средств для нагнетания страха, разжигания разногласий и роста неповиновения в рядах противника.

Воздействие на политических и военных лидеров, а также на руководителей (наиболее заметных представителей) СМИ, культуры и искусства про-

тивостоящей стороны является важным аспектом информационного противоборства в целом и психологических операций в частности. В этой связи в США особое внимание уделяется созданию коллективных и индивидуальных моделей поведения представителей высшего и среднего звена государственного и военного руководства, в частности составление психологических портретов на руководителей (в войсках — до командира соединения включительно).

Для изучения военачальников потенциального противника и составления их психологических портретов широко используются открытые источники, агентурные данные, а также мероприятия в рамках военного обмена, масштаб которого военно-политическое руководство США настойчиво стремится расширить.

Оперативная маскировка

Мероприятия по оперативной маскировке (в США этим термином обозначается дезинформация и введение противника в заблуждение) проводятся под руководством командующих объединенными группировками войск (сил). Их содержанием является оказание воздействия на органы принятия решений противника через его системы сбора, анализа и распределения информации путем предоставления им заведомо ложной информации и скрытия признаков реальной деятельности войск (сил). Цель этих мероприятий состоит в том, чтобы запутать, дезинформировать разведывательные органы противника, заставить их делать неправильные выводы и, как следствие, добиться от военного руководства противника неверных действий. Эти мероприятия позволяют также опередить противника в принятии решения, что является ключом к успеху любой операции.

Оперативная маскировка предполагает применение следующих способов:

- дезинформация - распространение заведомо ложной информации о составе, состоянии, дислокации, боеготовности своих войск, их группировках, характере и способах решения задач, планах, предназначении и состоянии военной техники и объектов;

- имитация - воспроизведение правдоподобных демаскирующих признаков, характерных для реальной деятельности войск (объектов), создание радиоэлектронной обстановки с использованием имитаторов, радиотехнических устройств, ложных сооружений и объектов, макетов военной техники и т. д.;

- демонстративные действия - преднамеренный показ противнику специально выделенными силами и средствами активной деятельности в целях его дезориентации и скрытия истинных намерений организаторов;

- обеспечение скрытности действий - определение признаков, распознаваемых разведывательными системами противника и позволяющих ему на основе их анализа получать особо важную и своевременную информацию; выбор и проведение мероприятий, которые обеспечивали бы скрытие этих

признаков и тем самым снижали бы до приемлемого уровня уязвимость союзников от действий разведки противника.

Мероприятия по оперативной маскировке обычно проводятся одновременно с другими, обеспечивающими действия объединенных сил. Планирование этих мероприятий осуществляется сверху — вниз с тем, чтобы планы по введению противника в заблуждение подчиненных звеньев поддерживали и обеспечивали аналогичные планы вышестоящего командования. В вышестоящем звене оно предполагает использование частей и подразделений самого нижнего уровня, хотя сами их командиры и их непосредственные начальники могут не знать содержания общего плана мероприятий. Поэтому в таких случаях важным является координация планов мероприятий по введению противника в заблуждение командиров нижестоящих частей и подразделений со старшим начальником.

Успех проведения мероприятий по оперативной маскировке в определяющей степени зависит от эффективности разведывательного обеспечения. Разведка в этом случае осуществляет вскрытие объектов противника, в отношении которых замышляются эти действия, оказывает помощь в разработке правдоподобной версии, предлагаемой для дезинформации, выборе наиболее перспективных объектов для реализации дезинформации и оценивает эффективность проведенных мероприятий.

Радиоэлектронная борьба

Радиоэлектронная борьба подразделяется на радиоэлектронное подавление, радиоэлектронную защиту и радиоэлектронное обеспечение. Радиоэлектронное подавление представляет собой действия наступательного характера, предпринимаемые с целью дезорганизовать, нейтрализовать или снизить возможности противника по эффективному использованию им радиоэлектронных систем в различных звеньях управления вооруженных сил. Радиоэлектронная защита предусматривает такие действия, как защита своих радиоэлектронных средств (РЭС) от помех, создаваемых противником, и осуществление контроля (наблюдения) за работой (РЭС) союзников, с целью исключения их взаимного влияния друг на друга. Радиоэлектронное обеспечение представляет собой действия, направленные на обнаружение, идентификацию и определение местоположения РЭС противника, которые могут являться как источниками получения разведданных, так и источниками информационных угроз.

При принятии решения об использовании средств радиоэлектронного подавления учитываются не только цели кампании или операции, но также и риск от возможных ответных действий противника. Для достижения максимального эффекта операции обязательным условием является тесная координация действий сил и средств РЭБ с другими мероприятиями по обеспечению информационных операций, проводимыми разведкой и связью.

Физическое уничтожение элементов информационной инфраструктуры рассматривается как проводимые в ходе ИО действия по применению

средств огневого поражения и физического уничтожения с целью вывода из строя ключевых элементов системы управления и связи противника.[6]

Воздействие на сети

Имеются данные, что ЦРУ, АНБ и военная разведка США изучают возможности и методы проникновения в компьютерные сети своих «потенциальных противников». Для чего, в частности, разрабатываются технологии внедрения электронных «вирусов», и «логических бомб», которые, не проявляя себя в мирное время, способны активизироваться по команде. И в случае кризисной ситуации, «электронные диверсанты» могут дезорганизовать оборонную систему управления, транспорт, энергетику, финансовую систему другого государства. Перспективными для таких целей считаются своего рода «зараженные» микросхемы, внедряемые в экспортируемую США вычислительную технику.

Средства ведения информационной войны в мирное время используются для сбора разведывательных данных, в том числе — путем несанкционированного доступа в компьютерные сети. При этом важно учесть, что в большинство стран оснащаются зарубежными, главным образом американскими программно-аппаратными комплексами. Здесь возможности иностранных спецслужб добывать из компьютерных сетей важную конфиденциальную информацию поистине велики.

Программно-математическое воздействие на компьютерные сети (компьютерная атака) определяется как действия с применением аппаратно - программных средств, направленные на использование, искажение, подмену или уничтожение информации, содержащейся в базах данных компьютеров и информационных сетей, а также на снижение эффективности функционирования либо вывод из строя самих компьютеров и компьютерных сетей.

Способы программно-математического воздействия по вполне понятным причинам не являются достоянием широкой гласности и описываются в специальной грифованной литературе, предназначенной для ограниченного круга заинтересованных лиц. Что касается средств такого воздействия, а работы в области их создания ведутся в США с 1990 года, то их можно подразделить на следующие:

- «Логические бомбы» - скрытые управляющие программы, которые по определенному сигналу или в установленное время приходят в действие, уничтожая или искажая информацию, воспрещая доступ к тем или иным важным фрагментам управляемого информационного ресурса либо дезорганизуя работу технических средств. В АСУ войсками и оружием подобное вмешательство даже в течение короткого времени может коренным образом повлиять на ход и исход боя, операции.

- Компьютерные вирусы, представляющие собой специализированные программные продукты, которые способны воспроизводить «логические бомбы» (обладая при этом еще большей разрушающей силой) и внедрять их дистанционно в информационные сети противника. Кроме того, вирусы спо-

собны самостоятельно размножаться, то есть копировать себя на магнитных носителях.

- Программные продукты типа «троянский конь» - программы, внедрение которых позволяет осуществлять скрытый несанкционированный доступ к информационному массиву противника для добывания разведданных.

- Нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения.

- Преднамеренно созданные, скрытые от обычного пользователя интерфейсы для входа в систему. Они, как правило, сознательно вводятся в программное обеспечение программистами-разработчиками с корыстными или диверсионно-подрывными целями.

- Малогабаритные устройства, способные генерировать электромагнитный импульс высокой мощности, обеспечивающий вывод из строя радиоэлектронной аппаратуры.

Кроме того, большое внимание уделяется созданию новых средств воздействия на системы связи, сбора и обработки информации. Так, с начала 90-х годов осуществляется переход к использованию не обнаруживаемых помех интеллектуального воздействия (блокировка ключевых элементов сообщения, например, названий и координат пунктов, времени действия с одновременным вводом ложных ключевых элементов). Такие системы базируются на автоматизированном анализе структуры сообщений, отслеживании ключевых слов, синтезировании речи в реальном масштабе времени.

В целом концепция информационного противоборства в том виде, в каком она реализуется в ВС США, не является новым понятием для российского военного искусства. Теоретические основы информационного противоборства достаточно полно раскрыты в российской военной науке через понятия «борьба с системами управления противника», «радиоэлектронная война», «завоевание господства в эфире», «психологическая война», «дезинформация», «военная хитрость» и т. п. «Новизна» американского подхода к теории информационного противоборства заключается в комплексном использовании военно-теоретических разработок по данной тематике и своих технологических достижений в области информатики.

В настоящее время США, обладая значительным преимуществом в области разработки и использования новейших радиоэлектронных систем и компьютерных технологий и основываясь на постулатах новой концепции, стремятся закрепить за собой доминирующую роль не только в политической, экономической и военной сферах, но и в мировой информационной инфраструктуре.

2. Порядок выполнения работы

Задание *1*. Изучить теоретический материал.

Задание *2.* Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы:

1. Требования по защите ИС и классы защиты ИС.
2. Положение о защите информации.
3. Безопасность глобальных сетевых технологий и методы информационного воздействия на глобальные информационные сети.
4. Правовые основы защиты информации и закон о защите информации.

Практическая работа №3

Влияние надежности цифровых подсистем на общую надежность электроэнергетических систем

Цель: рассмотреть влияние надежности цифровых подсистем, их кибербезопасности на общую надежность отдельных энергообъектов и электроэнергетических систем (ЭЭС) и их объединений.

Основы теории

Вопросы кибербезопасности современных электроэнергетических объектов, оснащенных цифровыми системами мониторинга, управления, релейной защиты и противоаварийной автоматики, становятся очень актуальными в виду новизны проблемы. На построенных в последние годы объектах, весь функционал устройств релейной защиты (РЗА), противоаварийной автоматики (ПА) и автоматизированного диспетчерского управления сосредотачивается на объединяемых единой цифровой информационной сетью компьютерных подсистемах энергообъекта: микропроцессорных терминалах РЗА и ПА, автоматических системах управления технологическими процессами (АСУ ТП).

Необходимо рассмотреть влияние надежности цифровых подсистем, их кибербезопасности на общую надежность отдельных энергообъектов и электроэнергетических систем (ЭЭС) и их объединений. В большинстве публикаций и нормативных документах, посвященных вопросам

кибербезопасности объектов электроэнергетики, основным способом ее обеспечения видится применение соответствующих технических средств, которые обеспечивают требуемую защиту от различных несанкционированных действий. Авторы, не отрицая необходимость применения специальных технических средств обеспечивающих кибербезопасность, предлагают сосредоточить внимание на человеческий фактор, как основную угрозу кибербезопасности, так как именно человек (сотрудник энергопредприятия, сотрудник поставщика и подрядчика, или стороннее лицо) является основной причиной потенциальной киберугрозы.

Надежность электроэнергетической системы обеспечивается двумя категориями. Первая – надежность функционирования всей производственной цепочки: производство электроэнергии, ее транспорт и распределение до электроустановок потребителей. Ключевая роль здесь отводится надежности основного электроэнергетического оборудования, которая обеспечивается соответствующими мероприятиями на этапах жизненного цикла (проектирования, производства, монтажа, наладки, эксплуатации).

Вторая – адекватность и эффективность управления. Известно, что функционирование ЭЭС возможно только при соответствующем непрерывном управлении, как отдельными электроустановками, так и ЭЭС вцелом.

Цифровые технологии, микропроцессорная техника со значительными вычислительными ресурсами позволяют создавать в рамках ЭЭС достаточно сложные и совершенные алгоритмы управления как в рамках оперативно-диспетчерского управления нормальными режимами, так и противоаварийного управления. Это в сочетании с новым поколением первичного оборудования, имеющим высокие эксплуатационные характеристики, и обладающим возможностями мониторинга и управления, позволяет повысить общую надежность ЭЭС.

С другой стороны, цифровым технологиям и микропроцессорной технике свойственна возможность резкого изменения своего функционала путем перепрограммирования, которая, при правильном применении, позволяет совершенствовать технологии и алгоритмы управления без замены оборудования. Но именно это и является основой новых видов угроз для ЭЭС – угроз кибербезопасности.

Киберугрозы по своей сути – это выполнение непредусмотренных функций: от несанкционированной передачи информации третьим лицам, до выполнения зловредных функций, что есть по сути частичный или полный отказ системы управления энергообъектом.

В качестве возможных угроз (возмущающих факторов) с позиции кибербезопасности для современных электроэнергетических объектов можно отметить следующие:

– невыявленные ошибки в программном обеспечении, вследствие чего информационные и управляющие системы энергообъекта работают по неверному алгоритму;

– злонамеренные программные дефекты (закладки), встроенные в программное обеспечение микропроцессорных устройств энергообъекта, с целью управляемого вывода из строя системы;

– кибератаки извне, через внешние цифровые каналы связи энергообъекта, путем перехвата каналов телемеханики и телеуправления, каналов общекорпоративного управления или встраивания зловредного программного кода в объектовые системы управления;

– ошибки оперативного и эксплуатационного персонала энергообъекта, которые приводят к снятию систем защиты внешних каналов связи, к замене программного обеспечения на непроектный вариант, к заражению вирусами и др.

Средствами повышения надежности и живучести являются:

– дублирование – установка нескольких одинаковых устройств;

– функциональное резервирование – реализация одинаковых или схожих функций с использованием разных физических и алгоритмических принципов;

– декомпозиция – разделение различных функций между разными устройствами, физическое разнесение кабелей и устройств;

– упрощение – применение простых, понятных и однозначных алгоритмов управления (снижается вероятность ошибок).

При переходе от традиционных энергообъектов к цифровым на основе МЭК-61850 происходит отказ от следующих принципов:

– отказ от функционального резервирования, т.к. коммуникационные сети (включая коммутаторы и маршрутизаторы), которые являются ключевыми в цифровых технологиях, работают на одном и том же принципе;

– отказ от декомпозиции, т.к. одни и те же коммуникационные сети (включая коммутаторы и маршрутизаторы), обеспечивающие шины процессов и шины объектов, выполняют функции доставки информации до всех устройств мониторинга и управления;

– отказ от упрощения, т.к. алгоритмы передачи и обработки цифровой информации по коммуникационным сетям сложны.

Для обеспечения надежности и живучести цифровых энергообъектов применяют только дублирование устройств, дублирование сетей и каналов связи, функциональное резервирование и декомпозицию исключительно на уровне прикладных электроэнергетических функций, но не на уровне цифровых технологий.

В тоже время, коммуникационные сети и микропроцессорные устройства цифровых энергообъектов универсальны, и без существенной модернизации могут решать любые информационные задачи, например, выполнять заведомо зловредные функции в процессе кибератаки, чего нельзя

сказать об устройствах на традиционных подстанциях (особенно на электромеханической базе).

Ключевыми элементами, которые могут быть подвержены кибератаке с последующим нарушением функционирования цифровой подстанции являются:

– коммуникационные сети энергообъекта, включая коммутаторы и маршрутизаторы;

– шины процессов и шины объектов (в соответствии с МЭК-61850), которые в цифровой подстанции являются неотъемлемыми элементами любой функции РЗА, ПА, мониторинга и оперативного управления;

– цифровые устройства РЗА, ПА, управления и мониторинга электрооборудованием;

– внешние цифровые каналы, по которым осуществляется технологическая и оперативная связь с другими энергообъектами и диспетчерскими пунктами.

Если все устройства РЗА, ПА, системы управления первичным оборудованием будут выполнены на цифровой базе и будут объединены в единую информационно-управляющую систему, то результатом кибератаки может быть полная потеря управляемости энергообъектом или заведомо ложное управление. В результате кибератаки возможна даже «перепрошивка» цифровых устройств или удаление на них системного и прикладного программного обеспечения. В последнем случае для восстановления работоспособности потребуется полный цикл пусконаладочных работ длительностью до нескольких месяцев.

Если несколько смежных подстанций подвергнется целенаправленной кибератаке, то вполне возможны случаи полного обесточивания значительной группы потребителей (включая ответственных). Также возможны случаи повреждения дорогостоящего первичного оборудования вследствие неустраненного КЗ или длительной неустраненной перегрузки.

При этом классические средства дальнего резервирования на смежных цифровых подстанциях могут быть также неработоспособны по все той же причине.

Традиционные подходы к кибербезопасности электроэнергетических объектов, в том числе, для цифровых подстанций, основаны на предположении о полной адекватности, квалифицированности, внимательности, дисциплинированности, честности, лояльности всех сотрудников, в том числе, производителей, проектировщиков, наладчиков и эксплуатационных организаций. Но, если активное сетевое оборудование и системы контроля доступа заведомо настроить неправильно, то с любой точки планеты можно будет буквально за несколько минут нарушить функционирование любого энергообъединения, даже такого масштабного, как ЕЭС России (ЕЭС/ОЭС). В традиционной энергетике, хотя бы расстояния между энергообъектами играли роль защитного барьера.

Можно отметить, что при построении цифровых подстанций на основе стандарта МЭК 61850 возникает системное противоречие: предлагается существенно упростить физическую (аппаратную) часть цифровой подстанции за счет принципиального усложнения алгоритмической и программной частей. Ослабление кибербезопасности и общей надежности цифровых энергообъектов, является неизбежным следствием увеличения объема универсального системного и коммуникационного программного обеспечения, которое раньше выполняло вспомогательные функции, а теперь станет ключевым элементом цифровой подстанции.

Поэтому можно констатировать, что проблема кибербезопасности объектов электроэнергетики становится ключевым элементом общей надежности ЭЭС. При этом в текущее время эта проблема явно недооценена и часто не принимается во внимание.

Как бы не совершенствовались в устойчивости к кибератакам программные и аппаратные средства, выполняющие прикладные и

коммуникационные функции на цифровых подстанциях, и какие бы дополнительные специальных технические средства не применялись для защиты от кибератак, все это не решает проблему человеческого фактора.

В нынешнее время вопросы кибербезопасности уже перешли из области только технических проблем, и перешли в область политики и межгосударственных отношений. При этом киберугрозы могут быть совершенно различными, при этом объектом первичных атак могут быть общекорпоративные информационные сети, которые в той иной степени соприкасаются с технологическими и производственными сетями.

Ключевой проблемой кибербезопасности является то, что одно и тоже устройство или программное обеспечение может быть настроено так, чтобы обеспечивать кибербезопасность и не допускать кибератаки, а может быть настроено по-другому, т.е. способствовать кибератакам. Внешний вид устройств при этом не меняется, однако их функциональность в части кибербезопасности принципиально разная. Отличие исключительно в настройках, причем отличаться может незначительное число параметров из тысячи совпадающих. Дилетант в вопросах кибербезопасности вообще не сможет выявить проблему путем каких-то периодических осмотров оборудования. Более того, есть риск создания уязвимостей как раз во время выполнения планово-предупредительных ремонтов, обслуживания, перенастройки и наладки оборудования. Поэтому, требуется привлечение специально обученных специалистов, которые способны решать задачи кибербезопасностина объектах электроэнергетики.

Вероятность целенаправленных кибератак зависит главным образом от двух составляющих: цены «услуг взлома» и масштаба последствий. Чем выше негативный масштаб последствий, тем большую цену будет готов заплатить потенциальный заказчик кибератаки. Электроэнергетика является ключевой инфраструктурной отраслью для современного государства и общества, является необходимой основой для

всех других инфраструктурных отраслей. Соответственно можно ожидать, что потенциальный заказчик может заплатить очень большую цену для решения своих задач (коммерческих или даже геополитических)

При большой цене за «услуги взлома» решающую роль будет играть лояльность специалистов. Соответственно, масштаб последствий, по сути, и определяет вероятность серьезной кибератаки.

Поэтому, важнейшим требованием к специалисту по кибербезопасности является требование правильного и добросовестного выполнения своих обязанностей. Однако, учитывая масштаб последствий, а также то, что заинтересованными сторонами в кибератаке могут быть иностранные государства, на первый план выходят вопросы политической и бизнес лояльности, патриотизма, эффективности спецслужб и т.п. То есть вопросы, выходящие за рамки техники и энергетики. Если ничего не предпринимать, то можно говорить о том, что любая цифровая подстанция должна превращаться в некий закрытый и секретный объект, наподобие военных и ядерных объектов, со всеми вытекающими затратами.

В реальности в настоящее время вообще полностью отсутствует какой-то значимый контроль на предмет кибербезопасности цифровых и программных прикладных технических средств в электроэнергетики. Максимум, что есть – это антивирусная защита компьютеров.

Поэтому с позиции надежности можно принимать возможность успешной кибератаки тем или иным способом как минимум: на одну технологическую подсистему, находящуюся в одной информационной сети; на один тип цифровых устройств/систем (если это связано с предусмотренной на заводе особенностью или невыявленной ошибкой); на все оборудование, обслуживаемое одним специалистом.

С учетом вышесказанного можно сделать вывод о том, что унификация и централизация приводит к снижению кибербезопасности, как минимум за счет потенциально возможного подкупа специалистов.

Соответственно повышение кибербезопасности, и как следствие общее повышение надежности (с позиции последствий кибератак) может быть обеспечено только за счет правильно организованной структуры управления в электроэнергетике. Когда единичный взлом или единичный подкуп специалистов не приводит к масштабной аварии в ЭЭС с серьезными, особенно долго устранимыми последствиями.

2. Порядок выполнения работы

Задание *1*. Изучить теоретический материал.

Задание *2*. Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы:

Поясните две категории, которыми обеспечивается надежность электроэнергетической системы.

1. Назовите возможные угрозы с позиции кибербезопасности для современных электроэнергетических объектов.

2. Перечислите средства повышения надежности и живучести.

3. Назовите ключевые элементы, которые могут быть подвержены кибератаке с последующим нарушением функционирования цифровой подстанции.

Практическая работа №4
Тема: Вредоносное программное обеспечение и методы борьбы

Цель: ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидности вирусов, способах заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов.

Основы теории

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной ".

Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или FAT-таблицу, "засоряет" оперативную память и т.д.).

Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно.

Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим

Проявление наличия вируса в работе на ПЭВМ

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Некоторые признаки заражения:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.
- операционная система не загружается;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- значительное увеличение количества файлов на диска;
- существенное уменьшение размера свободной оперативной памяти и т.п.

Некоторые виды вирусов вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере. Другие вирусы стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске.

Таким образом, если не предпринимать мер по защите от вируса, то последствия заражения компьютера могут быть очень серьезными.

Разновидности компьютерных вирусов

Вирусы классифицируют по среде обитания и по способу воздействия. По среде обитания вирусы подразделяются на следующие виды:

- файловые вирусы, которые внедряются главным образом в исполняемые файлы, т.е. файлы с расширением exe, com, bat, но могут распространяться и через файлы документов;
- загрузочные, которые внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
- макровирусы, которые заражают файлы-документы и шаблоны документов Word и Excel.;
- сетевые, распространяются по компьютерной сети;

По способу воздействия (особенностям алгоритма) вирусы отличаются большим разнообразием. Известны вирусы-паразиты, вирусы-черви, вирусы-невидимки (стелс-вирусы), вирусы-призраки (вирусы-мутанты), компаньон-вирусы, троянские кони и др.
Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков.
Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Рассмотрим "невидимые" и самомодифицирующиеся вирусы.

"Невидимые" вирусы. Многие резидентные вирусы (резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них) (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Разумеется, этот эффект наблюдается только на зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.
Самомодифицирующиеся вирусы. Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения, - модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью дизассемблеров нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры этой кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. Это, естественно, затрудняет нахождение таких вирусов программами-детекторами.
Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.
Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

- копирование информации - создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. Такая комбинация называется сигнатурой. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".
Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить

состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.
Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Программы-фильтры, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.
Однако преимущества использования программ-фильтров весьма значительны - они позволяют обнаружить многие вирусы на самой ранней стадии.

Программы-вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.
Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Рассмотрим структуру этой обороны.
Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.
На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков.
Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры.
Самый глубокий эшелон обороны - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные. В "стратегическом резерве" находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении.

Итак, одним из основных методов борьбы с вирусами является своевременная профилактика их появления и распространения. Только комплексные профилактические меры защиты обеспечивают защиту от возможной потери информации. В комплекс таких мер входят:

1. **Регулярное архивирование информации (создание резервных копий важных файлов и системных областей винчестера).**
2. **Использование только лицензионных дистрибутивных копий программных продуктов.**
3. **Систематическая проверка компьютера на наличие вирусов. Компьютер должен быть оснащен эффективным регулярно используемым и постоянно обновляемым пакетом антивирусных программ. Для обеспечения большей безопасности следует применять параллельно несколько антивирусных программ.**
4. **Осуществление входного контроля нового программного обеспечения, поступивших дискет. При переносе на компьютер файлов в архивированном виде после распаковки их также необходимо проверять.**
5. **При работе на других компьютерах всегда нужно защищать свои дискеты от записи в тех случаях, когда на них не планируется запись информации.**
6. **При поиске вирусов следует использовать заведомо чистую операционную систему, загруженную с дискеты.**
7. **При работе в сети необходимо использовать антивирусные программы для входного контроля всех файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютерным сетям.**

Современные технологии антивирусной защиты позволяют защитить от вируса файловые сервера, почтовые сервера и сервера приложений. Например, антивирус Касперского для защиты файловых серверов позволяет обнаружить и нейтрализовать все типы вредоносных программ на файловых серверах и серверах приложений, работающих под управлением ОС Solaris, включая "троянские" программы, Java и ActiveX – апплеты.

В состав антивируса Касперского для защиты файловых серверов входят:

- антивирусный сканер, осуществляющий антивирусную проверку всех доступных файловых систем на наличие вирусов по требованию пользователя. Проверяются в том числе архивированные и сжатые файлы;
- антивирусный демон, являющийся разновидностью антивирусного сканера с оптимизированной процедурой загрузки антивирусных баз в память, осуществляет проверку данных в масштабе реального времени;
- ревизор изменений, Kaspersky Inspector, отслеживает все изменения, происходящие в файловых системах компьютера. Модуль не требует

обновлений антивирусной базы: контроль осуществляется на основе снятия контрольных сумм файлов (CRC – сумм) и их последующего сравнения с данными, полученными после изменения файлов.

Комбинированное использование этих модулей позволяет создать антивирусную защиту, наиболее точно отвечающую системным требованиям. Обнаруженные подозрительные или инфицированные объекты могут быть помещены в предварительно указанную "карантинную" директорию для последующего анализа.
Антивирус Касперского обеспечивает полномасштабную централизованную антивирусную защиту почтовых систем, работающих под управлением ОС Solaris.
Проверке на наличие вирусов подвергаются все элементы электронного письма – тело, прикрепленные файлы (в том числе архивированные и компрессированные), внедренные OLE-объекты, сообщения любого уровня вложенности. Обнаруженные подозрительные или инфицированные объекты могут быть вылечены, удалены, переименованы, или помещены в заранее определенную карантинную директорию для последующего анализа.

Ежедневное обновление базы вирусных сигнатур, автоматически реализуется через Интернет при помощи специально встроенного модуля и обеспечивает высокий уровень детектирования компьютерных вирусов.

2. Порядок выполнения работы

Задание *1*. Изучить теоретический материал.

Задание *2*. Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы:

1. Биометрия. Технологии создания защищенных систем с помощью биометрии.
2. Угрозы, виды угроз и дифференциация угроз.
3. Методы несанкционированного доступа в локальные сети.
4. Модель нарушителя.
5. Угрозы. Классификация угроз. Активные и пассивные угрозы.
6. Спам. Защита от спама. Средства и технологии защиты от спама.

Практическая работа №5

Интернет угрозы и методы борьбы с ними

Цель: изучить основные закономерности возникновения и классификацию угроз информационной безопасности, пути и каналы утечки информации и методы борьбы с интернет угрозами.

Основы теории

Компьютерная преступность — это противоправная и осознанная деятельность образованных людей и, следовательно, наиболее опасная для общества. Итак, западными специалистами и экспертами констатируется крайне тяжелое положение с информационной безопасностью в финансовых структурах, их неспособность, противостоять возможным атакам на информационные системы

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Основные определения и критерии классификации угроз

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.

Чаще всего 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.

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

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат — как можно более оперативно.

Нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы суще-

ствует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Угрозы можно классифицировать по нескольким критериям:

· по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

· 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).

Угрозы могут быть как случайными, так и умышленными (преднамеренно создаваемыми).

К случайным угрозам относятся:

- ошибки обслуживающего персонала и пользователей:
- потеря информации, обусловленная неправильным хранением архивных данных;
- случайное уничтожение или изменение данных;
- сбои оборудования и электропитания:
- сбои кабельной системы;
- перебои электропитания;
- сбои дисковых систем;
- сбои систем архивирования данных;
- сбои работы серверов, рабочих станций, сетевых карт и т. д.
- некорректная работа программного обеспечения:
- изменение данных при ошибках в программном обеспечении;
- заражение системы компьютерными вирусами.
- несанкционированный доступ:
- случайное ознакомление с конфиденциальной информацией посторонних лиц.

К умышленным угрозам относятся:

- несанкционированный доступ к информации и сетевым ресурсам;
- раскрытие и модификация данных и программ, их копирование;
- раскрытие, модификация или подмена трафика вычислительной сети;
- разработка и распространение компьютерных вирусов, ввод в программное обеспечение логических бомб;
- кража магнитных носителей и расчетных документов;
- разрушение архивной информации или умышленное ее уничтожение;
- фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;

- перехват и ознакомление с информацией, передаваемой по каналам связи, и т. п.

В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

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.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь — следствие непреднамеренных ошибок.

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

· отказ пользователей;

· внутренний отказ информационной системы;

· отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

· нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

· невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

· невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

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 (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

· ошибки при (пере)конфигурировании системы;

· отказы программного и аппаратного обеспечения;

· разрушение данных;

· разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать 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.).

Весьма опасны так называемые «обиженные» сотрудники — нынешние и бывшие. Как правило, они стремятся нанести вред организации-«обидчику», например:

· испортить оборудование;

· встроить логическую бомбу, которая со временем разрушит программы и/или данные;

· удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия,- пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных «злоумышленников» (среди которых самый опасный — перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Некоторые примеры угроз доступности

Угрозы доступности могут выглядеть грубо — как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего — грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования — не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом — с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует все же признать надуманной.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении угроз конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем теперь к угрозам доступности, которые будут похитрее засоров канализации.

Речь пойдет о программных атаках на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно — полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное.

При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов — атака, получившая наименование «SYN-наводнение». Она представляет собой попытку переполнить таблицу «полуоткрытых» TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке «PapaSmurf» уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты «съедают» полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме — как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала «моды» на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее — владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре PentiumI дает возможность локальному пользователю путем выполнения определенной команды «подвесить» компьютер, так что помогает только аппаратный RESET.

Программа «Teardrop» удаленно «подвешивает» компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USAToday, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что

реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее мы проводили различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

· ввести неверные данные;

· изменить данные.

Из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя (мы приводили соответствующие примеры). Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

Еще один урок: угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить «неотказуемость», компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного ПО — пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности — частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую — и не может быть обеспечена) необходимая защита. Угроза же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна — осуществить доступ к данным в тот момент, когда они наименее защищены.

Перехват данных — очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются… выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной сети выставки — это слишком суровое испытание честности всех участников. Еще один пример изменения, о котором часто забывают, — хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад — выполнение действий под видом лица, обладающего полномочиями для доступа к данным (см., например, статью Айрэ Винклера «Задание: шпионаж» в JetInfo, 1996, 19).

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример — нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

2. Порядок выполнения работы

Задание *1*. Изучить теоретический материал.

Задание *2*. Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы:

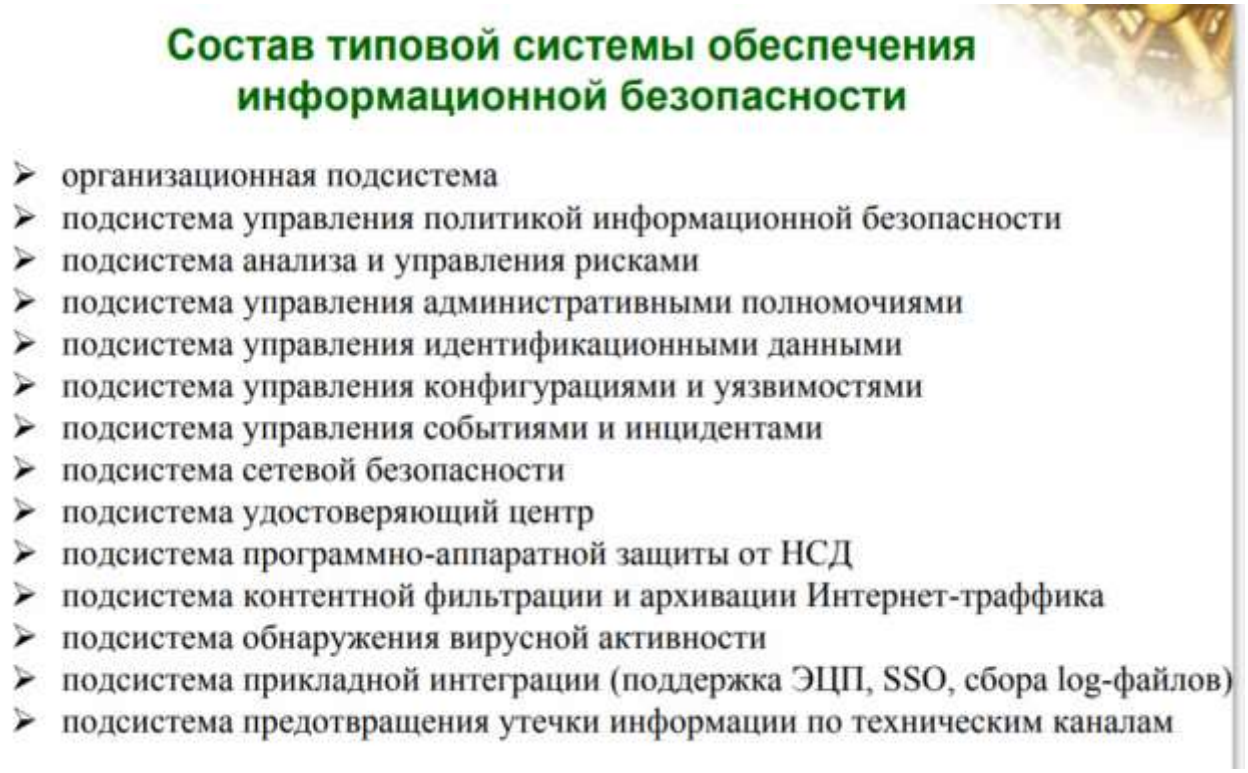
1. Правовые основы защиты информации и закон о защите информации.
2. Международные документы и стандарты в области информационной безопасности.
3. Классы каналов несанкционированного получения информации
4. Основные свойства информации. Важность, полнота, адекватность, релевантность

Практическая работа №6

Тема: Современные системы управления информационной безопасностью

Цель: изучить основы создания систем управления информационной безопасностью.

1. Краткое теоретическое описание



2. Порядок выполнения работы

Задание *1*. Изучить лекционный материал по соответствующей теме.

Задание *2.* Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы:

1. Антивирусы и антивирусная защита. Классификация вредоносных программ.
2. Межсетевые экраны и методы создания защищенных систем, включающих межсетевые экраны.
3. Особенности защиты различных операционных систем.
4. Аппаратные средства защиты информации.
5. Протоколы PPP, SMTP, FTP и методы создания защищенного обмена
6. Что такое информация?
7. Понятие информационной безопасности.
8. Обеспечение безопасности при работе с электронной почтой.
9. Резервирование информации. Средства создания резервных копий.
10. Что такое «криптография»?
11. Физическое разрушение информационных систем и методы защиты от физического воздействия.
12. Троянские кони, люки и технология салями.
13. Технология VPN. Построение защищенных каналов связи.

Практическая работа №7
Тема: Электронно-цифровая подпись. Система удостоверяющих центров. Сертификаты.

Цель: изучить виды и технологии электронно-цифровых подписей.

Основы теории

Электронная подпись предназначена для защиты электронного документа, передаваемого посредством различных сред или хранящегося в цифровом виде, от подделки и является атрибутом электронного документа. Она получается в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяет идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе.

Электроная подпись (ЭП) - это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ

Электронная подпись используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью.

Электронный документ - это любой документ, созданный при помощи компьютерных технологий и хранящийся на носителях информации, обрабатываемых при помощи компьютерной техники, будь то письмо, контракт или финансовый документ, схема, чертеж, рисунок или фотография.

Использование ЭП позволяет:

- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;
- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;
- гарантировать достоверность документации;
- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;
- построить корпоративную систему обмена документами.

Подделать ЭП невозможно - это требует огромного количества вычислений, которые не могут быть реализованы при современном уровне математики и вычислительной техники за приемлемое время, то есть пока информация, содержащаяся в подписанном документе, сохраняет актуальность. Дополни-

тельная защита от подделки обеспечивается сертификацией Удостоверяющим центром открытого ключа подписи.
С использованием ЭП работа по схеме "разработка проекта в электронном виде - создание бумажной копии для подписи - пересылка бумажной копии с подписью - рассмотрение бумажной копии - перенос ее в электронном виде на компьютер" уходит в прошлое.

Электронные подписи разделяются законом 2011 г. на три вида.

- **Простые подписи** создаются с помощью кодов, паролей и других инструментов, которые позволяют идентифицировать автора документа, но не позволяют проверить его на предмет наличия изменений с момента подписания.
- **Усиленная неквалифицированная подпись** создана с использованием криптографических средств и позволяет определить не только автора документа, но проверить его на наличие изменений. Для создания таких подписей может использоваться сертификат неаккредитованного центра, можно также вообще обойтись без сертификата, если технические средства позволяют выполнить требования закона.
- **Усиленная квалифицированная подпись** является разновидностью усиленных, она имеет сертификат от аккредитованного центра и создана с помощью подтвержденных ФСБ средств.

Простые и неквалифицированные подписи заменяют подписанный бумажный документ в случаях, оговоренных законом или по согласию сторон. Например, простые подписи могут использовать граждане для отправки сообщений органам власти. Усиленная подпись также может рассматриваться как аналог документа с печатью.

Квалифицированные подписи заменяют бумажные документы во всех случаях, за исключением тех, когда закон требует наличие исключительно документа на бумаге. Например, с помощью таких подписей граждане могут получать госуслуги в электронном виде, а органы государственной власти могут отправлять сообщения гражданам и взаимодействовать друг с другом через информационные системы. Ранее выданные сертификаты ЭЦП и подписанные с их помощью документы приравниваются к квалифицированным подписям.

Иностранные электронные подписи приравниваются в России к тем видам подписей, которым они соответствуют.

Простая электронная подпись, в отличие от прежней электронно-цифровой подписи, не предназначена для защиты документа от подделки. Она не позволяет обнаружить возможное искажение содержания документа.

Единственная ее функция — подтверждение факта формирования электронной подписи (а не самого документа!) определенным лицом.

Целям определения лица, подписавшего электронный документ, а также обнаружения факта внесения изменений в документ после его подписания служит усиленная электронная подпись. Именно эта подпись (в двух видах — неквалифицированная и квалифицированная) является аналогом прежней электронной цифровой подписи.

Поскольку простая электронная подпись требует использования кодов, паролей или иных средств, станет ясно, что можно считать электронной подписью, а что нет. Очевидно, что в случае электронного письма роль электронной подписи не может играть имя отправителя, вручную поставленное после текста, так как оно никак не зависит от пароля, используя который отправитель сформировал и отправил письмо. Информацией, указывающей на лицо, от имени которого был послан документ, может служить, вероятно, идентификатор сообщения в сочетании с IP-адресом компьютера отправителя, свидетельствующие о том, что сообщение было создано в результате доступа к почтовой системе, сопровождавшегося вводом пароля, принадлежащего определенному пользователю. Электронный адрес отправителя и имя отправителя можно считать подписью лишь в том случае, если оператор информационной системы обеспечивает их достоверность, ведь почтовый протокол позволяет указывать любое имя и любой обратный адрес, и некоторые почтовые системы не накладывают здесь никаких ограничений.

Средствами ЭЦП являются аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи,
- подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе,
- создание закрытых и открытых ключей электронных цифровых подписей.

В основе электронной подписи лежит криптография открытого ключа. С ее помощью формируется специальный сертификат пользователя. Он содержит данные о пользователе, открытый ключ и электронную подпись сертификата, ее можно проверить с помощью открытого ключа удостоверяющего центра. Алгоритм гарантирует, что произвести генерацию подписи может только удостоверяющий центр, который имеет секретный ключ шифрования и доверие к которому является основой для работы всей системы ЭЦП.

Доверие к удостоверяющим центрам основано на иерархическом принципе: сертификат удостоверяющего центра нижнего уровня заверяется элек-

тронной подписью удостоверяющего центра более высокого уровня. Высочайшим уровнем удостоверяющих центров является федеральный, который находится под управлением государственных органов. Вся система доверия, построенная на сертификатах, образует так называемую инфраструктуру открытых ключей (Public Key Infrastructure, PKI). При такой инфраструктуре требуется проверка не только легитимности ключа удостоверяющего центра, выдавшего сертификат, но и всех вышестоящих удостоверяющих центров. В частности, при формировании электронной транзакции необходимо проверить не только математическую корректность ЭЦП, но и валидность всей цепочки сертификатов, задействованных при изготовлении сертификата подписанта, на момент подписания им конкретного электронного документа.

В России сейчас создается система PKI, которая доступна практически всем желающим. Изначально она была создана агентством Росинформтехнологии на базе Общероссийского государственного информационного центра (ОГИЦ). Однако сейчас федеральный удостоверяющий центр передан в ведение «Ростелекома». Этот телекоммуникационный оператор активно предлагает развивать различные проекты с использованием PKI.

2. Порядок выполнения работы

Задание *1.* Изучить теоретический материал.

Задание *2.* Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы:

1. Сертификаты. Протокол HTTPS. Центры сертификации.
2. Понятие информации в контексте информационной безопасности.
3. Виды информации.
4. Что такое «СПАМ»?
5. Информационные системы, использующие технологии ЭЦП
6. ЭЦП. Роль ЭЦП в современном обществе. Технология ЭЦП.

Практическая работа №8
Моделирование угроз кибербезопасности

Цель: Изучение угроз кибербезопасности. Моделирование угроз.

Основы теории

Моделирование угроз кибербезопасности

Основой управления информационной безопасностью предприятия является анализ рисков. Фактически риск представляет собой интегральную оценку того, насколько эф-

фективно существующие средства защиты способны противостоять информационным атакам.

Обычно выделяют две основные группы методов расчёта рисков безопасности. Первая группа позволяет установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности. В качестве источников таких требований могут выступать:

Нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности;

Требования действующего российского законодательства - руководящие документы ФСТЭК (Гостехкомиссии), СТР-К, требования ФСБ РФ, ГОСТы и др.;

Рекомендации международных стандартов - ISO 17799, OCTAVE, CoBIT и др.;

Рекомендации компаний-производителей программного и аппаратного обеспечения - Microsoft, Oracle, Cisco и др.

Рис. Источники требований информационной безопасности, на основе которых может проводиться оценка рисков

Вторая группа методов оценки рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита.

Методы первой и второй группы могут использовать количественные или качественные шкалы для определения величины риска информационной безопасности. В первом случае риск и все его параметры выражаются в числовых значениях. Так, например, при использовании количественных шкал вероятность проведения атаки может выражаться числом в интервале , а ущерб атаки может задаваться в виде денежного эквивалента материальных потерь, которые может понести организация в случае успешного проведения атаки. При использовании качественных шкал числовые значения заменяются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определённый интервал количественной шкалы оценки. Количество уровней может варьироваться в зависимости от применяемых методик оценки рисков. В таблицах 3.1 и 3.2 приведены примеры качественных шкал оценки рисков информационной безопасности, в которых для оценки уровней ущерба и вероятности атаки используется пять понятийных уровней.

Таблица 3.1. Качественная шкала оценки уровня ущерба

№	Уровень ущерба	Описание

1	Малый ущерб	Приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании
2	Умеренный ущерб	Вызывает заметные потери материальных активов или к умеренному влиянию на репутацию компании
3	Ущерб средней тяжести	Приводит к существенным потерям материальных активов или значительному урону репутации компании
4	Большой ущерб	Вызывает большие потери материальных активов и наносит большой урон репутации компании
5	Критический ущерб	Приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке, что делает невозможным дальнейшую деятельность организации

При использовании качественных шкал для вычисления уровня риска применяются специальные таблицы, в которых в первом столбце задаются понятийные уровни ущерба, а в первой строке - уровни вероятности атаки. Ячейки же таблицы, расположенные на пересечении первой строки и столбца, содержат уровень риска безопасности. Размерность таблицы зависит от количества концептуальных уровней вероятности атаки и ущерба. Пример таблицы, на основе которой можно определить уровень риска, приведён в табл. 3.3.

Таблица 3.2. Качественная шкала оценки вероятности проведения атаки

№	Уровень вероятности атаки	Описание
1	Очень низкая	Атака практически никогда не будет проведена. Уровень соответствует числовому интервалу вероятности [0, 0.25)
2	Низкая	Вероятность проведения атаки достаточно низкая. Уровень соответствует числовому интервалу вероятности [0.25, 0.5)
3	Средняя	Вероятность проведения атаки приблизительно равна 0,5
4	Высокая	Атака скорее всего будет проведена. Уровень соответствует числовому интервалу вероятности (0.5, 0.75]

5	Очень высокая	Атака почти наверняка будет проведена. Уровень соответствует числовому интервалу вероятности (0.75, 1]

Таблица 3.3. Пример таблицы определения уровня риска информационной безопасности

Вероятность атаки	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Ущерб					
Малый ущерб	Низкий Риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Умеренный ущерб	Низкий Риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Ущерб средней тяжести	Низкий Риск	Средний риск	Средний риск	Средний риск	Высокий риск
Большой ущерб	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
Критический ущерб	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

При расчете значений вероятности проведения атаки, а также уровня возможного ущерба могут использоваться статистические методы, методы экспертных оценок или элементы теории принятия решений. Статистические методы предполагают анализ уже накопленных данных о реально случавшихся инцидентах, связанных с нарушением информационной безопасности. На основе результатов такого анализа строятся предположения о вероятности проведения атак и уровнях ущерба от них в других АС. Однако применение статистических методов не всегда возможно из-за отсутствия в полном объёме статистических данных о ранее проведённых атаках на информационные ресурсы АС, аналогичной той, которая выступает в качестве объекта оценки.

При использовании аппарата экспертных оценок проводится анализ результатов работы группы экспертов, компетентных в области информационной безопасности, которые на основе имеющегося у них опыта определяют количественные или качественные уровни риска. Элементы теории принятия решений позволяют применять для вычисления значения риска безопасности более сложные алгоритмы обработки результатов работы группы экспертов.

В процессе анализа рисков информационной безопасности могут использоваться специализированные программные комплексы, позволяющие автоматизировать процесс анализа исходных данных и расчёта значений рисков. Примерами таких комплексов являются "Гриф" и "Кондор" (компании "Digital Security"), британский CRAMM (компания Insight Consulting, подразделение Siemens), американский RiskWatch (компания RiskWatch), а также "АванГард" (Института Системного Анализа РАН).

Традиционно выделяют три основные составляющие безопасности информации:

конфиденциальность (confidentiality) - сохранение информации в тайне, невозможность раскрытия информации без согласия заинтересованных сторон;

целостность (integrity) - непротиворечивость и правильность информации, защита информации от неавторизованной модификации;

доступность (availability) - обеспечение наличия информации и работоспособности основных услуг для пользователя в нужное для него время.

Ведутся дискуссии на тему полноты " триады CIA " для описания угроз ИБ. Существует альтернатива этой классификации - т.н. " гексада Паркера " (Parkerian Hexad). Помимо вышеперечисленных свойств, Дон Паркер выделяет:

подлинность (authenticity) - в применении к пользователю определяет соответствие участника взаимодействия своему имени; в применении к сообщению - достоверность того, что данные были созданы заявленным источником.

управляемость, или владение (possession or control) - гарантия того, что законный владелец является единственным лицом, во власти которого изменить информацию или получить к ней доступ на чтение

полезность (utility) - "практичность", удобство доступа; нахождение информации в такой форме, что ее законный владелец не должен для получения доступа тратить неоправданных усилий (таких, как преобразование формата, подбор ключа шифрования и т.д.)

Существует также классификация 5A, горячо одобряемая известным криптографом Брюсом Шнайером:

Authentication (аутентификация: кто ты?)

Authorization (авторизация: что тебе можно делать?)

Availability (доступность: можно ли получить работать с данными?)

Authenticity (подлинность: не повреждены ли данные злоумышленником?)

Admissibility (допустимость: являются ли данные достоверными, актуальными и полезными?)

Мы в данном курсе будем придерживаться модели угроз STRIDE, являющейся компонентом используемой Microsoft методологии SDL (Secure Development Lifecycle).

Spoofing (притворство)

Tampering (изменение)

Repudiation (отказ от ответственности)

Information Disclosure (утечка данных)

Denial of Service (отказ в обслуживании)

Elevation of Privilege (захват привилегий)

Данная классификация расширяет традиционный подход к оценке безопасности информации (покрытие области CIA обеспечивают компоненты Tampering + Information Disclosure + Denial of Service) и позволяет разработчику взглянуть на информационную систему с позиции злоумышленника. Далее мы будем рассматривать продукты и технологии, упорядочивая их согласно тому, от какого типа угрозы по классификации STRIDE они призваны защитить информационные ресурсы.

Краткие итоги

В данной лекции были рассмотрены принципы применения анализа рисков для управления информационной безопасностью предприятия. Проведен сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, Гексада Паркера, 5A, STRIDE.

2. Порядок выполнения работы

Задание *1*. Изучить теоретический материал.

Задание *2.* Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы

1. Анализ рисков как основа управления кибербезопасностью.
2. Модель угроз STRIDE.
3. Инструменты анализа и контроля информационных рисков.
4. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, STRIDE.

Практическая работа №9
Экономическая эффективность средств обеспечения информационной безопасности

Цель: изучить инструменты оценки экономической эффективности средств информационной безопасности

Основы теории

Важность подчеркивал В.Мамыкин, директор по информационной безопасности кабинета президента Microsoft в России и СНГ, в своих выступлениях на конференциях Security @ Interop '2008 и IT-Summit'2008 [7.48]. Согласно [7.49], большинство зарубежных компаний (84%) используют ROI и другие инструменты для оценки инвестиций в ИБ, которые составляют в среднем 5% всего ИТ-бюджета. В России на ИБ идет 0,5% ИТ бюджета, т.е. в 10 раз меньше. Такую ситуацию В.Мамыкин напрямую связывает с тем, что в нашей стране пока не получила широкого распространения практика оценки эффективности средств обеспечения ИБ с экономических позиций.

Расчет финансово-экономических показателей СЗИ позволяет решить следующие задачи:

Обоснование внедрения системы по обеспечению информационной безопасности на предприятии с экономической точки зрения;

Оценка экономической эффективности внедрения или замены системы безопасности информации;

Прогнозирование расходов по созданию/ функционированию/ модернизации СЗИ (задача управления бюджетом);

Сравнение по экономическим критериям нескольких вариантов создания СЗИ, построенных на различных архитектурах (системах и компонентах), с целью выбора оптимального варианта реализации проекта (задача выбора ИТ-стратегии).

Качество информации, необходимой для принятия решения о целесообразности инвестиций, в первую очередь, будет зависеть от исходных данных, на основе которых производились вычисления. Уязвимым местом в любой методике расчета является именно сбор и обработка первичных данных, их качество и достоверность. Одним из основных вопросов является оценка затрат на ИБ. Выбор необходимой степени защиты должен учитывать ряд критериев: уровень секретности информации; ее стоимость; время, в течение которого она должна оставаться в тайне и т.д. Известный криптограф Брюс Шнайер (Bruce Schneier) в работе [7.26] подчеркивает, что термин "безопасность" лишен смысла без сведений о том, от кого и на какой срок защищена информация. Это утверждение

применимо как к системам обеспечения безопасности в целом, так и к их важнейшему компоненту - средствам криптографической защиты информации.

Средства криптографической защиты информации (СКЗИ) представляют собой средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности. Росс Андерсон (Ross J Anderson), ведущий эксперт в области информационной безопасности, в своей статье [7.3] приходит к выводу, что при оценке уровня защищенности специалист должен принимать во внимание не только технические характеристикикриптосистемы, получаемые путем криптоанализа и анализа информационных потоков, но использовать также и экономические инструменты.

Рассмотрим возможность разработки методики анализа эффективности СКЗИ с учетом того, каким угрозам защищаемая информация будет подвергаться со стороны злоумышленников.

Для решения поставленной задачи необходимо:

формализовать процесс оценки эффективности криптографической защиты;

разработать математическую модель угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств;

обеспечить криптоаналитика набором инструментальных средств, позволяющих оценить стойкость криптографических средств по отношению к идентифицированным угрозам;

провести анализ существующих методов оценки СКЗИ с экономических позиций и выбрать финансово-экономические показатели, подходящие для экономической оценки инвестиций в СКЗИ.

Поставленные цели согласуются с задачами, вошедшими в перечень основных направлений и приоритетных проблем научных исследований в области информационной безопасности Российской Федерации, который был разработан секцией по информационной безопасности Научного совета при Совете Безопасности Российской Федерации при активном участии ведущих ученых и специалистов научных учреждений и организаций РАН, вузов, федеральных органов исполнительной власти, работающих в различных областях, связанных с обеспечением национальной безопасности (см. [7.44], пп. 46, 47 и 56).

Процесс оценки эффективности криптографической защиты

Анализ существующих подходов

При оценке эффективности СКЗИ важнейшим критерием считается криптостойкость, т.е. способность противостоять атакам криптоаналитика [7.40]. Такой подход не учитывает других важных требований к криптосистемам, а именно (см. [7.46]):

минимальный объем используемой ключевой информации;

минимальная сложность реализации (в количестве машинных операций);

стоимость;

высокое быстродействие.

Кроме того, использование СКЗИ, обеспечивающих устойчивость к взлому ниже некоторой "фоновой" вероятности, является экономически неоправданным [7.35]. Например, если вероятность выхода компании из бизнеса равна 230 (менее чем один из миллиона), то есть ли смысл для защиты информации, которая может нанести компании ущерб, сопоставимый с кризисом рынка, использовать алгоритм, вероятность вскрытия которого за приемлемое время составляет 2100?

В статье В.П.Иванова [7.38] эффективность криптографических средств защиты предлагается оценивать с использованием математического аппарата теории массового обслуживания и теории катастроф на основе вероятностно-временной группы показателей, в числе которых:

среднее время безопасного функционирования защищаемой системы;

время безопасного функционирования защищаемой системы с вероятностью НСД не выше заданной;

экономическая эффективность созданной системы защиты информации.

Выбор показателей эффективности представляет интерес, однако методика имеет ряд критических недостатков, которые делают невозможным ее применение на практике для оценки современных СКЗИ. В первую очередь это границы применимости: методика подходит только для оценки криптосистем, принадлежащих по классификации Ж.Брассара (Gilles Brassard) [7.6] к классу криптосистем ограниченного использования, стойкость которых основывается на сохранении в секрете алгоритмов зашифрования и расшифрования. Однако, согласно фундаментальному допущению Кирхгоффа (Auguste Kerckhoffs) [7.14], стойкость криптосистемы должна основываться не на секретности алгоритмов зашифрования и расшифрования, а на секретности некоторого значения, которое называется ее ключом. Все современные криптосистемы построены по этому принципу, и исследования их надежности всегда должны проводиться в предположении, что потенциальному противнику о криптосистеме известно все, за исключением используемого ключа.

Еще одним недостатком методики, описанной в работе [7.38], является то, что она не учитывает зависимости эффективности криптосистемы от условий ее использования. Очевидно, эффективность одной и той же криптосистемы в разных контекстах может существенно отличаться, т.к. среда функционирования системы накладывает определенные ограничения на возможные сценарии атак.

Существуют методики, позволяющие построить модели угроз и уязвимостейинформационных систем и на основе анализа рисков получить количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты (см., например, [7.39]):

метод CRAMM, разработанный Агентством по компьютерам и телекоммуникациям Великобритании по заданию Британского правительства [7.9];

семейство программных продуктовRiskWatch от одноименной американской компании [7.23];

комплексная система анализа и управления рискамиинформационной системы ГРИФ, созданная отечественной компанией Digital Security [7.10].

Эти инструментальные средства полезны специалисту при проведении аудита систем обеспечения безопасности предприятия, однако они не учитывают специфики СКЗИ и, как показано в [7.34], не подходят для решения поставленной в данной работе задачи.

Наконец, существуют методы формального анализа криптопротоколов. Криптографический протокол [7.24] регламентирует последовательность действий, выполняемых двумя и более сторонами для решения какой-либо задачи с использованием криптографических преобразований и алгоритмов. Можно выделить три основных класса методов анализа криптопротоколов:

Дедуктивные методы, основанные на автоматическом доказательстве теорем, связанных со свойствами исследуемого криптопротокола [7.5];

Методы анализа состояний, моделирующие криптопротокол в виде конечного автомата [7.4];

Методы статического анализа, объектом исследования в которых являются потоки данных и управления [7.7].

Перечисленные подходы имеют существенный недостаток: все они построены на предположении, что используемые в протоколе криптографические примитивы идеальны. Рассматривается только концептуальная схема протокола, от конкретных методов шифрования и их подверженности атакамзлоумышленника принято абстрагироваться.

Модель процесса оценки эффективности СКЗИ

Наиболее эффективным при выборе и оценке криптографической системы считается использование экспертных оценок [7.46]. При оценке эффективности СКЗИ необходимо принимать во внимание взаимосвязь факторов, определяющих ее подверженность атаке определенного типа. Упрощенное графическое представление модели сценария атаки изображено на рис. 7.1. Во избежание избыточности из модели исключен элемент "Защищаемые ресурсы", который задается неявно - через элемент "Злоумышленник" (характер зашифрованной информации определяет возможных злоумышленников, которые могут осуществлять попытки взлома в целях нарушения конфиденциальности, целостности или доступности).

Рис. 7.1. Модель сценария взлома

На основании предложенной модели сценария атаки построена модель угроз безопасности информационных ресурсов из трех элементов [7.30] - ABC-модель ("A" от англ. Attack - атака, "B" от англ. code-Breaker - взломщик шифра, "C" от англ. Cryptosystem - криптосистема). Математическое описание ABC -модели дано позже, здесь мы рассмотрим процесс экспертной оценки эффективности криптографической защиты (графическая модель процесса изображена на рис. 7.2).

Целью этапов 1-3 является построение ABC -модели. Первый этап - определение объекта исследования. Здесь описываются конкретные характеристики криптосистемы. На втором этапе задаются параметры, определяющие тип потенциальных взломщиков криптосистемы. Как будет показано в следующем разделе, при наличии формальных представлений исследуемой криптосистемы и потенциальных злоумышленников мы можем перейти к третьему этапу, т.е. определить типы атак, которым подвержена криптосистема, а также связанный с ними риск.

Четвертый этап представляет собой анализ устойчивостикриптосистемы к атакам, определенным на третьем этапе. Для проведения криптоанализа специалиста необходимо обеспечить набором инструментальных средств, исследование и разработке которых будет рассмотрена далее.

Наконец, пятый этап предполагает использование различных подходов к оценке экономической эффективности инвестиций в СКЗИ на основании данных, полученных на этапах 1-4.

Рис. 7.2. Процесс оценки эффективности криптографической защиты

Моделирование угроз безопасности информационных ресурсов

Задача состоит в разработке АВС -модели угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств, которая даст возможность формализовать взаимосвязь между параметрами криптосистемы, потенциальных злоумышленников и возможных атак. Для решения поставленной задачи необходимо:

Разработать многокритериальные классификационные схемы, позволяющие идентифицировать:

криптосистему - с учетом особенностей ее реализации;

потенциального взломщика - с учетом его мотивации, возможностей и квалификации;

криптоаналитическую атаку - с учетом применимости к различным криптосистемам и необходимых для ее осуществления ресурсов.

На основе разработанных классификаций создать параметрические модели криптосистем, атак и злоумышленников;

Установить зависимость возможных сценариев взлома от характеристик злоумышленников и от особенностей реализации исследуемой криптосистемы.

Анализ существующих подходов

Для идентификации исследуемой криптосистемы нужно выделить набор ее ключевых свойств. Известны классификации криптосистем, в числе которых - классификационная схема, предложенная швейцарским математиком и криптографом У.Маурером (Ueli Maurer) [7.21] и основанная на том, чтобы различать криптосистемы по количеству ключей, упомянутая выше схема Ж.Брассара [7.6], в которой криптосистемы различаются в зависимости от сохранения в секрете механизма шифрования. Ни одна из этих классификаций сама по себе не позволит идентифицироватькриптосистему - необходима многокритериальная классификация. С этой точки зрения представляет интерес работа К.Черезова [7.43], в которой предлагаются обобщающие критерии для сравнения продуктов на российском рынке СКЗИ:

Фирма-производитель;

Тип реализации;

Наличие действующих сертификатов соответствия ФСБ России и классы защиты;

Реализованные криптографические алгоритмы;

Поддерживаемые операционные системы;

Предоставляемый программный интерфейс;

Наличие реализации протокола SSL / TLS ;

Поддерживаемые типы ключевых носителей;

Интегрированность с продуктами и решениями компании Microsoft ;

Наличие дистрибутива продукта в свободном доступе на сайте производителя, дилерской сети распространения и сервиса поддержки.

Недостатком приведенной классификации для построения параметрической модели криптосистемы является то, что для решения поставленной в нашей работе задачи важны не "потребительские" и "технические" характеристики СКЗИ, а их свойства, определяющие подверженность тем или иным атакам.

Типы взломщиков, от которых криптосистема должна обеспечить защиту, определяют разумный уровень безопасности. Чтобы понять, каким атакам будет подвергаться система, необходимо выделить наиболее вероятных взломщиков. Классификации Дж.Говарда (John D Howard) [7.13] и Б.Шнайера [7.25], в которых злоумышленники различаются в зависимости от их движущих мотивов, подходят для высокоуровневого анализа контекста использования криптосистемы, однако не позволяют установить зависимость возможных сценариев атак от характеристик злоумышленников.

Существует большое количество классификаций и таксономийатак. Недостатком схем, описанных в [7.15, 7.17, 7.22, 7.28], является то, что они разработаны для описания атак на компьютерные системы, а объектом нашего исследования является более узкий класс атак - криптоаналитические атаки. Классификация Кирхгоффа [7.14] по доступу к открытому и зашифрованному тексту с появлением атак по побочным каналам [7.37] уже не может считаться полной; кроме того, она не позволяет учитывать такие важные факторы, как объем необходимых ресурсов, возможность распараллеливания и т.д.

Математическая модель угроз безопасности информационных ресурсов

На основе анализа существующих классификационных схем, перечисленных выше, нами были разработаны новые многокритериальные классификации криптосистем, атак и злоумышленников (см. рис. 7.3 - 7.5). Далее мы покажем, как применение разработанных классификационных схем для построения АВС -модели позволяет провести всесторонний анализ угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств.

Пусть $A \subseteq A_1 \times A_2 \times \ldots \times A_8$- множество параметрических моделей атак, где A_i ($i = \overline{1,9}$) - множество значений i-го параметра модели атаки, определяющего тип атаки в соответствии с критериями разработанной классификации. Каждая модель $\vec{a} \in A$ представляет собой вектор $(a_1, a_2, \ldots, a_9)$, где $\vec{a_i} \in A_i$.

Аналогично, параметрическая модель злоумышленника задается в виде вектора $\vec{b} \in B$, где $B \subseteq B_1 \times B_2 \times \ldots \times B_6$, B_j ($j = \overline{1,6}$) - множество значений j-го параметра модели злоумышленника, модель криптосистемы - $\vec{c} \in C$, где $C \subseteq C_1 \times C_2 \times \ldots \times C_6, C_k$ ($k = \overline{1,6}$) - множество значений k-го параметра модели криптосистемы в соответствии с многокритериальной классификацией. Заметим, что множества значений параметров модели атаки, злоумышленника и криптосистемы конечны.

При дальнейшем изложении для краткости слово "модель" применительно к модели атаки, модели злоумышленника и модели криптосистемы будем опускать.

С каждой атакой будем связывать значение риска, вычисляемое по общеизвестной формуле на основе двух факторов - вероятности происшествия и тяжести возможных последствий:

Риск = Влияние Вероятность

Обозначим через $\Re : A \times B \times C \to [0;1]$ функцию, задающую уровень риска, связанного с атакой $\vec{a} \in A$ в условиях, когда она может быть применена злоумышленником $\vec{b} \in B$ для взлома криптосистемы $\vec{c} \in C$.

Пусть $I : C \times A \to [0;1]$ - функция влияния (от англ. impact - влияние, воздействие). Под влиянием мы будем понимать степень ущерба от применения атаки $\vec{a} \in A$ к криптосистеме $\vec{c} \in C$.

Пусть $P : B \times A \to [0;1]$ - вероятность того, что злоумышленник $\vec{b} \in B$ предпримет атаку $\vec{a} \in A$, т.е. обладает ресурсами для ее осуществления и сочтет эту атаку целесообразной.

Тогда функция риска $\Re$ выражается следующим образом:

$$\Re(\vec{a}, \vec{b}, \vec{c}) = I(\vec{c}, \vec{a}) * P(\vec{b}, \vec{a})$$

Определим функцию $I(\vec{c}, \vec{a})$. Для этого рассмотрим семейство функций $I_{gh} : C_g \times A_h \to R_+$, , , где R_+ - множество неотрицательных действительных чисел. Здесь функция I_{gh} задает уровень взаимного влияния параметра криптосистемы C_g и параметра атаки a_h :

$I_{gh}(c, a) = 0$, если атака со значением параметра $a \in A_h$ не применима к криптосистеме со значением параметра $c \in C_g$;

$0 < I_{gh}(c, a) < 1$, если значение параметра криптосистемы $c \in C_g$ снижает вероятность успешного применения атаки со значением параметра $a \in A_h$;

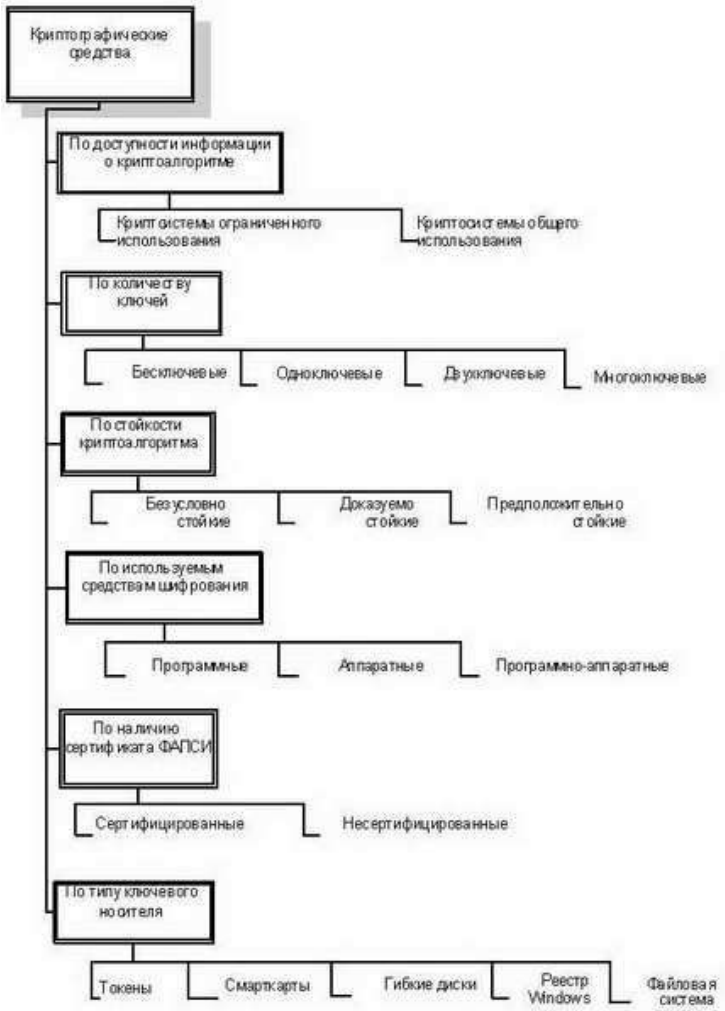


Рис. 7.3. Классификация криптосистем

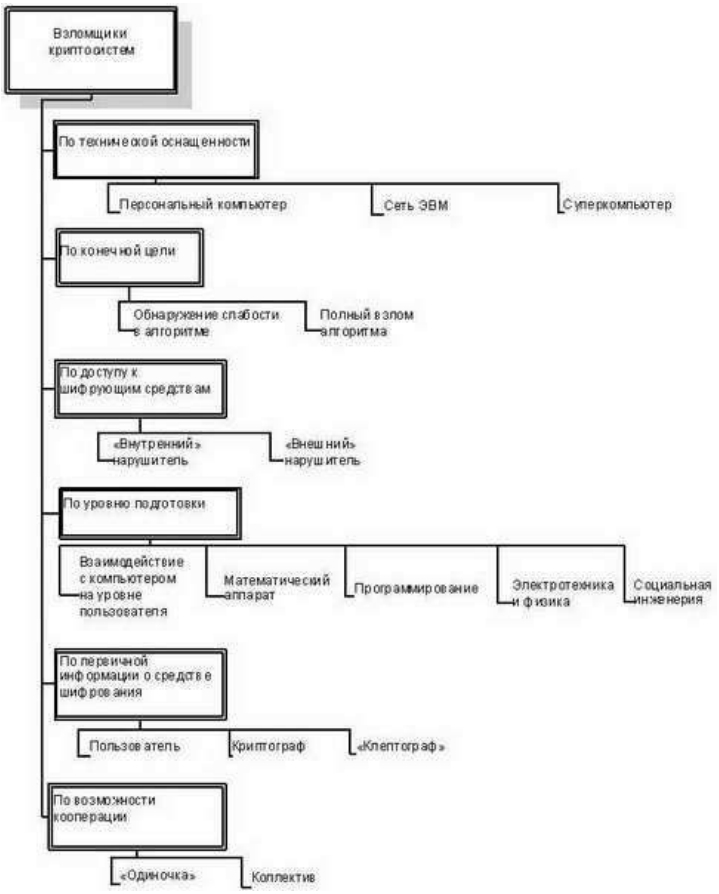


Рис. 7.4. Классификация злоумышленников

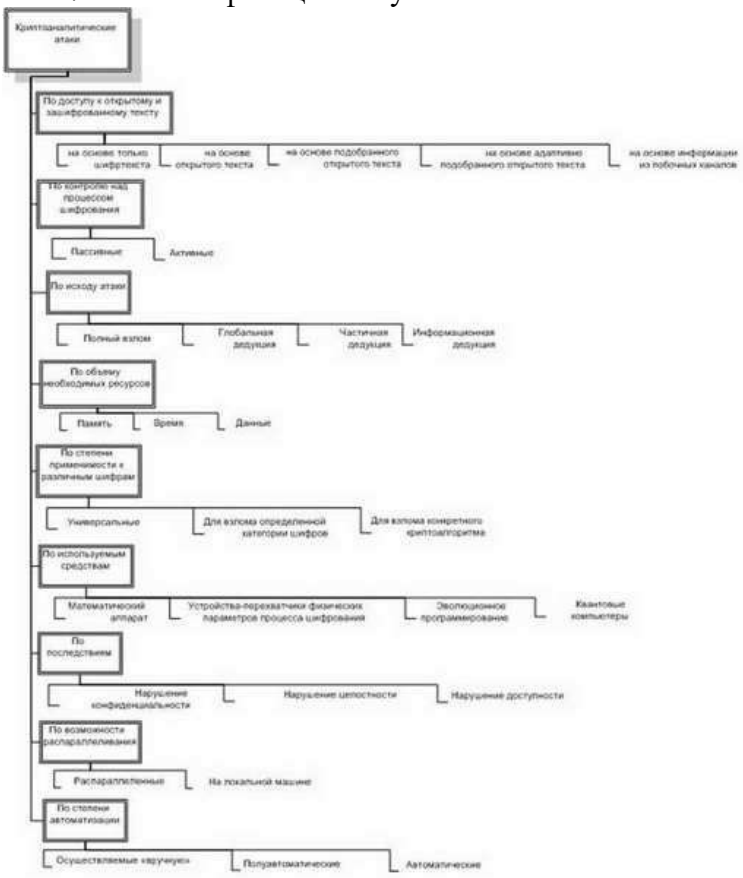


Рис. 7.5. Классификация криптоатак

$I_{gh}(c,a)=1$, если значение параметра криптосистемы $c \in C_g$ не влияет на применимость атаки с параметром $a \in A_h$;

$I_{gh}(c,a)>1$, если значение параметра криптосистемы $c \in C_g$ указывает на то, что атака с параметром $a \in A_h$ применима для ее взлома.

Например, если исследуемый алгоритм шифрования реализован в аппаратном обеспечении, это повышает вероятность применения для взлома криптосистемыатак по побочным каналам [7.37] (это вид криптографических атак, использующих информацию, которая может быть получена с устройства шифрования и не является при этом ни открытым текстом, ни шифртекстом). Уровень взаимного влияния параметров криптосистемы и атаки определяется на основе экспертных оценок.

Обозначим через $\overline{I_{gh}} : C_g \times A_h \to [0;1]$ нормированную функцию:

$$\overline{I_{gh}}(c,a)=\frac{I_{gh}(c,a)}{\sum_{\xi \in C_g} I_{gh}(\xi,a)}$$

Тогда уровень ущерба от применения атаки $\vec{a} \in A$ к криптосистеме $\vec{c} \in C$ вычисляется по следующей формуле:

$$I(\vec{c},\vec{a})=\min_{h=\overline{1,9}} \prod_{g=1,5} \overline{I_{gh}}(c_g,a_h)$$

,

где атака и криптосистема заданы параметрами $(a_1,a_2,\ldots,a_9)$ и $(c_1,c_2,\ldots,c_6)$ соответственно. Заметим, что уровень влияния всех параметров криптосистемы на применимость атаки с заданным значением -го параметра в этой формуле $\prod_{g=1}^{6} \overline{I_{gh}}(c_g,a_h)$ вычисляется по мультипликативному критерию: . Если значение хотя бы одного из параметров криптосистемы противоречит возможности применения атаки, то результатом оценки применимости атаки к криптосистеме будет нулевое значение, что соответствует нулевому уровню ущерба от атаки.

Функция $P(\vec{b},\vec{a})$, определяющая зависимость между параметрами $(a_1,a_2,\ldots,a_9)$ атаки и $(b_1,b_2,\ldots,b_6)$ злоумышленника, выражается аналогично функции $I(\vec{c},\vec{a})$. В качестве иллюстрации взаимосвязи параметров злоумышленника и атаки можно привести следующий пример: наличие у предполагаемого взломщика доступа к распределенным вычислительным ресурсам повышает вероятность применения метода "грубой силы" и, вообще говоря, любой атаки, легко поддающейся распараллеливанию.

Таким образом, общая формула для определения уровня риска, связанного с атакой $\vec{a} \in A$ в условиях, когда эта атака может быть применена злоумышленником $\vec{b} \in B$ для взлома криптосистемы $\vec{c} \in C$, имеет вид:

$$\Re(\vec{a},\vec{b},\vec{c})=\min_{h=\overline{1,9}} \prod_{g=\overline{1,6}} \overline{I_{gh}}(c_g,a_h) * \min_{h=\overline{1,9}} \prod_{t=\overline{1,6}} \overline{P_{th}}(b_t,a_h)$$

Будем считать, что криптосистема $\vec{c} \in C$ подвержена атаке $\vec{a} \in A$ в условиях, когда ей угрожает злоумышленник $\vec{b} \in B$, если $\Re(\vec{a}, \vec{b}, \vec{c}) > \theta$, т.е. связанный с ней уровень риска превышает заданное пороговое значение θ, где $\theta \in [0; 1]$. Допустимый уровень риска θ является настраиваемым параметром ABC -модели угрозкриптосистемы. Значение θ задается с учетом двух критериев:

критичности защищаемых данных;

временных и других ресурсов, доступных специалисту, который осуществляет аудит системы.

В общем случае:

криптосистема может включать несколько подсистем (например, генератор ключей и симметричный шифратор), к каждой из которых применим свой набор атак;

на криптосистему может нападать несколько злоумышленников.

Множество атак, которым подвержена криптосистема, состоящая из подсистем $\vec{c} \in C'$ ($C' \subseteq C$), в условиях, когда ей угрожают злоумышленники $\vec{b} \in B'$ ($B' \subseteq B$), будем определять по формуле $\Lambda = \cup_{\vec{b} \in B'} \cup_{\vec{c} \in C'} \lambda(\vec{b}, \vec{c})$, где $\lambda(\vec{b}, \vec{c}) = \{\vec{a} \in A : \Re(\vec{a}, \vec{b}, \vec{c}) > \theta\}$ при заданном уровне риска. Для оценки защищенности криптосистемы необходимо с использованием инструментальных средств оценить ее способность противостоять атакам, входящим в множество Λ.

В описанной математической модели сделаны следующие допущения:

не учитывается зависимость параметров атаки от сочетания параметров криптосистемы, хотя влияние каждого параметра принимается во внимание;

не учитывается возможность совместных действий со стороны взломщиков различных типов, хотя можно задать модель нападения со стороны однородного коллектива злоумышленников.

Исправление ABC -модели с учетом указанных допущений привело бы к ее значительному усложнению. Вопрос о том, насколько эти допущения снижают точность моделирования угроз безопасности, подлежит дальнейшим исследованиям.

Важно отметить, что разработанная классификационная схема для построения моделей атак на алгоритмы шифрования с небольшими модификациями применима и для моделирования атак на криптопротоколы. Возможность использования ABC -модели угроз для комплексного исследования криптосистемы является важной, т.к. вопрос совместного функционирования криптопротоколов и шифров в рамках одной криптосистемы, как показано в [7.27], до сих пор был мало изучен.

Оценка стойкости криптографических средств к идентифицированным угрозам

После того, как выделен набор атак, представляющих наибольшую угрозу для защищаемых данных, необходимо оценить способность криптосистемы противостоять этим атакам.

Базой для получения таких оценок может служить статистика взлома и успешных атак на криптосистемы. Например, известно, что стартовавший в 1997 г. на сайте www.distributed.net проект "распределенного взлома" RC5-64 (блочного шифра компании RSA, использующего 64-битный ключ) [7.29], в котором на добровольной основе приняли участие более 300 тысяч пользователей глобальной сети, был успешно завершен за пять лет (1757 дней) - за это время было перебрано 85% всего пространства ключей. Однако такая информация, во-первых, не всегда доступна, а, во-вторых, со временем теряет актуальность, т.к. повышение производительности вычислительной техники и появление новых видов атак на шифры ведет к понижению стойкости известных криптографических

алгоритмов. Для проверки надежности шифров, используемых в криптосистеме, специалисту необходим набор инструментальных средств, позволяющих осуществлять криптоанализ и не предполагающих у использующего их специалиста наличия глубоких знаний в программировании или электротехнике. В качестве примера можно привести упомянутые в п.1.1 автоматизированные средства анализа криптопротоколов [7.7] или прототип программного комплекса для моделирования атак по побочным каналам [7.37], описанный в [7.19]. Моделирование аппаратного обеспечения в работе [7.19 осуществляется с использованием SystemC [7.2] - языка проектирования и верификации моделей системного уровня, реализованного в виде библиотеки на C++ с открытым исходным кодом. На примере программных и аппаратных реализаций шифраAES показано, каким образом разработанный инструмент позволяет обнаружить уязвимости в реализации криптографического алгоритма.

Особого внимания заслуживают асимметричные криптосистемы. Функциональные возможности шифров с открытым ключом используются в разнообразных технологиях, в числе которых [7.33]:

Управление идентичностью;

Цифровая подпись кода;

Доверенная платформа;

Управление авторством;

Построение VPN ;

Гарантированное уничтожение информации;

Защита от физической кражи носителя информации.

Процесс криптоанализа асимметричных шифров сопряжен с решением задач из теории чисел и общей алгебры, т.к. практически все используемые алгоритмы асимметричной криптографии основаны проблемах факторизации и дискретного логарифмирования в различных алгебраических структурах. Чтобы определить, могут ли математические задачи той или иной размерности считаться достаточно прочным фундаментом для криптографических целей, специалисту требуются инструментальные средства, позволяющие оценивать быстродействие алгоритмов факторизации и дискретного логарифмирования. Необходимо учитывать, что криптоаналитик может не обладать навыками в области программирования. Кроме того, важно предусмотреть возможность работы под управлением наиболее распространенной ОС - MS Windows.

Итак, выделим набор основных требований к инструментальным средствам криптоанализа:

Эффективность вычислений с длинными числами в модулярной арифметике;

Наличие алгоритмов работы с разреженными матрицами;

Наличие алгоритмов создания факторной базы, решета и разложения на множители;

Удобство пользовательского интерфейса;

Возможность сборки в ОС Windows.

Будем считать, что решение соответствует поставленной задаче, если оно удовлетворяет всем перечисленным пяти критериям оценки.

Анализ существующих подходов

Математические пакеты Maple [7.36] и Mathematica [7.45] отличаются простотой кодирования алгоритмов и не имеют встроенных ограничений на разрядность операндов. Тем не менее, помимо платформенной зависимости они обладают критическим недостатком - низкой эффективностью теоретико-числовых операций.

Высокой эффективности можно добиться, используя встроенные средства низкоуровневого языка программирования для разработки функций, необходимых для исследования криптосистем. Однако важно отметить, что реализация примитивов для конструи-

рования современных методов криптоанализа асимметричных шифров оперирует числами в длинной арифметике. Встроенные числовые типы языков C и C++ имеют ограниченную разрядность:

long: 32 бита;

long long: 64 бита;

double: 53 бита - мантисса, 11 бит - экспонента;

long double: в зависимости от реализации языка может быть определен как double (см. выше) либо как extended double: 64 бита - мантисса, 15 бит - экспонента [7.1].

В реализации языков на платформе . NET отсутствует тип extended double: он доступен только неявно при выполнении промежуточных вычислений (например, где умножение дает результат, выходящий за пределы диапазона значений double, но последующее деление возвращает промежуточный результат обратно в этот диапазон). Кроме того, существует встроенный 128-битный тип данныхdecimal, позволяющий представлять целые числа разрядностью до 96 бит (в соответствии с размером мантиссы), однако он реализуется в режиме эмуляции, поскольку аппаратная поддержка этого типа на сегодняшний день отсутствует [7.11].

Java поддерживает возможность работы с длинными числами и обладает переносимостью, однако недостатком является низкая эффективность реализации.

Рассмотрим специализированные библиотеки функций для работы с длинной арифметикой и теоретико-числовыми задачами, находящиеся в открытом доступе: LIP, LiDIA, CLN, GMP, NTL.

Библиотека для работы с длинной арифметикойLIP (Long Integer Package) [7.18] является одной из первых таких библиотек. Она была разработана на языке ANSIC известным специалистом Арженом Ленстрой (Arjen K. Lenstra) и поддерживается Полом Лейлендом (Paul Leyland). При хорошей переносимости эта библиотека обладает низкой эффективностью. Кроме того, в ней отсутствует поддержка высокоуровневых теоретико-числовых алгоритмов.

Библиотека CLN (a Class Library for Numbers) [7.8] реализует элементарные арифметические, логические и трансцендентные функции. Авторами библиотеки являются Бруно Хейбл (Bruno Haible) и Ричард Крекел (Richard Kreckel). CLN содержит большой набор классов, реализованных на C++, в частности, классы для поддержки модулярной арифметики, операций с целыми, рациональными и комплексными числами, числами с плавающей запятой. Поскольку числовая библиотека задумывалась как универсальная, это привело к ее ограниченной применимости для решения узкоспециализированных задач.

Библиотека теоретико-числовых алгоритмов LiDIA [7.16], предложенная Томасом Папаниколау (Thomas Papanikolau, Technical University of Darmstadt), написана на C++,поддерживает различные пакеты для работы с целыми числами (GMP, CLN, LIP) и характеризуется высокоэффективными реализациями типов данных с увеличенной точностью и алгоритмов с большой временной сложностью. Недостатком библиотеки LiDIA является невозможность сборки в операционных системах Windows, что очень существенно в связи с широким использованием продуктов Microsoft и необходимостью проверки их защищенности.

При разработке GMP (GNU Multiple Precision arithmetic library) [7.12] был сделан упор на скорость. Эффективность от использования библиотеки теоретико-числовых алгоритмов GMP растет при увеличении разрядностиоперандов. Часть функций реализована на языке C, часть - на ассемблере. Автором является Торбжорд Гранланд (Torbjord Granlund). Помимо несовместимости с платформой Windows, недостатком GMP является отсутствие алгоритмов формирования факторной базы, разложения на множители и ряда других, необходимых для реализации современных методов криптоанализа.

Таблица 7.1. Сравнительный анализ программных решений для решения задач криптоанализа

Решение / Критерии оценки	Mathematica	LIP	CLN	LiDIA	GMP	NTL	КРИПТО
Эффективность вычислений	-	-	-	+	+	+	+
Возможность сборки в ОС Windows	+	+	+	-	-	+	+
Наличие алгоритмов работы с разреженными матрицами	-	-	-	+	+	-	+
Наличие алгоритмов создания факторной базы, решета и разложения на множители	-	-	-	+	-	-	+
Удобство пользовательского интерфейса	+	-	-	-	-	-	+

Известная математическая библиотека библиотека NTL (a Library for doing Number Theory) [7.20] разработана Виктором Шаупом (Victor Shoup) для поддержки теоретико-числовых алгоритмов. Функции, реализованные на языке C++,характеризуются переносимостью. Библиотеку можно использовать совместно с GMP в целях повышения эффективности. NTL имеет большое количество преимуществ по сравнению с рассмотренными аналогами (см. табл. 7.1), однако для решения поставленной задачи реализованных в библиотеке NTL алгоритмов недостаточно. Кроме того, для ее использования в криптоанализе специалист должен обладать квалификацией программиста.

Как видно из табл. 7.1, ни одно из рассмотренных решений не удовлетворяет одновременно всем пяти установленным критериям.

Инструментальные средства криптоанализа асимметричных шифров

Для оценки стойкости криптосистем аналитику необходим инструмент, эффективно работающий с теоретико-числовыми задачами, обладающий простым пользовательским интерфейсом и легко расширяемый. Прототип такого средства для криптоанализа систем с открытым ключом реализован в виде программного комплекса "Инструментальные средства криптоанализа асимметричных шифров" (обозначение в таблице - КРИПТО) [7.31, 7.32]. Программный комплекс состоит из библиотеки КОНСТРУКТОР, включающей необходимые примитивы для конструирования современных методов криптоанализа асимметричных шифров, и приложения АНАЛИТИК, имеющего графический интерфейс пользователя для доступа алгоритмам факторизации и дискретного логарифмирования с использованием функций библиотеки КОНСТРУКТОР. Библиотека КОНСТРУКТОР написана на языке C++ и содержит компоненты, реализующие следующие основные функции:

Дискретное логарифмирование;

Факторизация целых чисел;

Тестирование чисел на простоту;

Решение систем линейных уравнений в кольцах вычетов и конечных полях.

Для выполнения операций с длинными числами использована библиотека NTL. Выбор базовой библиотеки, обусловленный её функциональностью, скоростью, компактностью (исходный код занимает чуть более 600 килобайт) и переносимостью, позволил получить эффективные реализации перечисленных теоретико-числовых алгоритмов. В настоящей работе мы не будем приводить полное сравнение библиотеки КОНСТРУКТОР

с аналогами; заметим лишь, что если на решение задачи дискретного логарифмирования размерностью 55 бит с использованием системы Maple уходит порядка 8 часов, то разработанный программный комплекс КРИПТО позволяет за 10 минут вычислить дискретный логарифм в поле разрядностью 80 бит (испытания проводились на компьютере со следующими аппаратными характеристиками: процессор Intel Pentium IV 3,20GHz, ОЗУ 1Гб).

Расчет эффективности капитальных вложений в использование криптографических средств

Оценки вероятности взлома криптосистемы за определенный период позволяют определить сокращение риска НСД к данным от использования криптосистемы, например, за 1-й год - на 95%, за 2-й год - на 70%, за 3-й год - на 35%. При наличии достоверных оценок объема потерь от реализации угроз нарушения конфиденциальности, целостности или доступности защищаемых данных можно получить математические ожидания потерь и использовать их для определения эффективности криптосистемы с экономических позиций.

Анализ существующих подходов

В настоящее время нет единых стандартов, позволяющих оценить СКЗИ с экономических позиций, поэтому любой из разработанных методов заслуживает отдельного рассмотрения с выявлением его положительных и отрицательных сторон, а также сравнения его с другими представителями этого класса. В табл. 7.2 представлены результаты сравнительного анализа методов оценки эффективности инвестиций в средства обеспечения ИБ. На основании результатов был сделан вывод, что оптимальным является метод дисконтирования денежных потоков [7.42], позволяющий получить наиболее полное представление о целесообразности капитальных вложений, хотя и требующий много времени и усилий на расчет экономических показателей.

Методика дисконтирования денежных потоков при оценке эффективности инвестиций в СКЗИ

Определим денежные потоки, связанные с использованием СКЗИ, за период t (где t = 0, 1, 2…. T - периоды, T - горизонт расчета).

С защищаемой информацией связаны значения дохода $Profit_t$ от ее использования и ущерба $Loss_t$ от НСД в течение указанного промежутка времени t. Затраты $Cost_t$ на приобретение, установку и эксплуатацию СКЗИ могут быть определены очень точно. Пусть результаты оценки способности криптосистемы противостоять атакам показали, что в t-м периоде злоумышленник получит доступ к защищаемой информации с вероятностью P_t. Тогда математическое ожидание дохода R_t, связанного с использованием оцениваемой СКЗИ, вычисляется по формуле:

$$R_t = -Cost_t + Profit_t * (1 - P_t) - Loss_t * P_t$$

На основании этих данных о притоках и оттоках денежных средств вычисляются финансово-экономические показатели эффективности инвестиций в криптосистему и делаются выводы о ее соответствии потребностям организации.

Таблица 7.2. Сравнительный анализ методов оценки эффективности инвестиций в средства обеспечения ИБ

Методика оценки	Преимущества	Недостатки
Коэффициент возврата инвестиций	Показатель, понятный финансистам.	Отсутствие достоверных методов расчета в области ИТ. "Статичный" показатель.

Совокупная стоимость владения	Позволяет оценить целесообразность реализации проекта на основании оценки только затрат. Предполагает оценку затрат на различных этапах всего жизненного цикла системы.	Не учитывает качество системы безопасности. "Статичный" показатель. Показатель, специфичный для ИТ.
Дисконтированные показатели эффективности инвестиций	Показатель, понятный финансистам. Учитывает зависимость потока денежных средств от времени. Учитывает все потоки денежных средств, связанные с реализацией проекта.	Сложность расчета.

2. Порядок выполнения работы

Задание *1*. Изучить теоретический материал.

Задание *2*. Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, ответы на контрольные вопросы

Контрольные вопросы

1. Оценка средств криптозащиты.
2. Экономическое обоснование расходов на обеспечение персональной кибербезопасности.
3. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности.
4. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности.

5. Учебно-методическое и информационное обеспечение дисциплины

Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Перечень основной литературы:

1. Влацкая И.В., Заельская Н.А., Надточий Н.С. Проектирование и реализация прикладного программного обеспечения / Учебное пособие.- Оренбург: Оренбургский государственный университет, 2015, http://www.iprbookshop.ru/54145.html

2. Карташевский В.Г., Лихтциндер Б.Я., Киреева Н.В., Буранова М.А. Компьютерные сети/ Учебник.- Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016, http://www.iprbookshop.ru/71846.html

Перечень дополнительной литературы:

1. Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия / Учебное пособие.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, http://www.iprbookshop.ru/52217
2. Басалова Г.В. Основы криптографии / Учебное пособие.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, http://www.iprbookshop.ru/52158
3. Скрипник Д.А. Обеспечение безопасности персональных данных / учебное пособие.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, режим доступа http://www.iprbookshop.ru/52153

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. «Университетская библиотека онлайн» - http://biblioclub.ru
2. «Электронно-библиотечная система IPRbooks» http://www.iprbookshop.ru

Информационные справочные системы:

1	https://www.consultant.ru/ Консультатнт плюс - информационно-правовая система

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по организации и проведению самостоятельной работы
по дисциплине «Информационная безопасность в электроэнергетике»
для студентов направления подготовки
13.03.02 Электроэнергетика и электротехника

Содержание

Введение

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов в ВУЗе является важным видом учебной и научной деятельности студента.

Ведущая цель организации и осуществления СРС должна совпадать с целью обучения студента – подготовкой бакалавра с высшим образованием. При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности.

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

1. ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩЕГОСЯ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭЛЕКТРОЭНЕРГЕТИКЕ»

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения. В связи с этим, обучение в ВУЗе включает в себя две, практически одинаковые по объему и взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому СРС должна стать эффективной и целенаправленной работой студента.

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет

наличие у выпускников определенных способностей и умения самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной финансовой ситуации. Формирование такого умения происходит в течение всего периода обучения через участие студентов в практических занятиях, выполнение контрольных заданий и тестов, написание курсовых и выпускных квалификационных работ. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Ведущая цель организации и осуществления СРС должна совпадать с целью обучения студента – подготовкой специалиста и бакалавра с высшим образованием. При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности.

Формы самостоятельной работы студентов разнообразны. В соответствии с рабочей программой дисциплины «Электромагнитная совместимость в электроэнергетических системах» предусмотрены следующие виды самостоятельной работы студента:

- самостоятельное изучение литературы;
- выполнение контрольной работы
- выполнение индивидуальных творческих заданий.

Цель самостоятельного изучения литературы – самостоятельное овладение знаниями, опытом исследовательской деятельности.

Задачами самостоятельного изучения литературы являются:

- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов.

В результате освоения дисциплины формируются следующие компетенции:

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-1 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-1$_{ОПК-1}$ Понимает особенности работы современных информационных технологий	Определяет основные угрозы безопасности при использовании информационных технологий. Решает поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности.

1. ПЛАН-ГРАФИК ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
Очная форма обучения 4 семестр					
ОПК-1 ИД-1 $о_{ПК-1}$	Самостоятельное изучение литературы по темам №1-18	Собеседование	23,94	2,66	26,6
	Подготовка к лекциям	Собеседование	4,86	0,54	5,4
	Подготовка к практическим работам	Собеседование	36	4	40
		Итого:	**64,8**	**7,2**	**72**

Заочная форма обучения
4 семестр

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
4 семестр					
ОПК-1 ИД-1 $о_{ПК-1}$	Самостоятельное изучение литературы по темам №1-18	Собеседование	52,92	5,88	58,8
	Подготовка к лекциям	Собеседование	1,08	0,12	1,2
	Подготовка к практическим работам	Собеседование	36	4	40
		Итого:	**90**	**10,0**	**100**

3.КОНТРОЛЬНЫЕ ТОЧКИ И ВИДЫ ОТЧЕТНОСТИ ПО НИМ

В рамках рейтинговой системы успеваемость студентов по каждой дисци-

плине оценивается в ходе текущего контроля и промежуточной аттестации.

При проведении текущего контроля рейтинговая оценка знаний студента оценивается следующим образом:

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
1.	Моделирование угроз кибербезопасности	6 неделя	10
2.	Современные системы управления информационной безопасностью	11 неделя	15
3.	Влияние надежности цифровых подсистем на общую надежность электроэнергетических систем	16 неделя	30
	Итого за 4 семестр		**55**
	Итого		**55**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	**Рейтинговый балл (в % от максимального балла за контрольное задание)**
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

Типовые контрольные задания и иные материалы, характеризующие этапы формирования компетенций

Вопросы для собеседования

1. Понятие национальной безопасности, виды безопасности.
2. Информационная безопасность в системе национальной безопасности Российской Федерации.
3. Доктрина безопасности РФ. Национальные и международные документы в области защиты информации.
4. Физическая защита информационных систем. Программные средства защиты информации.
5. Этапы создания систем защиты информации.
6. Защита информации. Основные принципы обеспечения информационной безопасности.
7. Терминологические основы информационной безопасности. Основные понятия и определения.

8. Конфиденциальность, целостность, доступность. Требования по защите ИС и классы защиты ИС.
9. Положение о защите информации. Безопасность глобальных сетевых технологий и методы информационного воздействия на глобальные информационные сети.
10. Правовые основы защиты информации и закон о защите информации.
11. Общеметодологические принципы теории информационной безопасности.
12. Комплексность. Этапы развития информационной безопасности:
13. Системы безопасности ресурса;
14. Этап развитой защиты; Этап комплексной защиты.
15. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
16. Комплексность: целевая, инструментальная, структурная, функциональная, временная.
17. Угрозы. Классификация и анализ угроз информационной безопасности. подверженность физическому искажению или уничтожению;
18. Возможность несанкционированной (случайной или злоумышленной) модификации; опасность несанкционированного получения информации лицами, для которых она не предназначена.
19. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.
20. Методы и средства обеспечения информационной безопасности.
21. Методы нарушения конфиденциальности, целостности и доступности информации.
22. Причины нарушения целостности информации
23. Потенциально возможные злоумышленные действий в автоматизированных системах обработки данных.
24. Функции и задачи защиты информации. Методы формирования функций защиты.
25. Скрытие информации о средствах, комплексах, объектах и системах обработки информации.
26. Дезинформация противника. Легендирование.
27. Введение избыточности элементов системы. Резервирование элементов системы.
28. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации.
29. Маскировка информации. Регистрация сведений.

30. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования.
31. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности.
32. Защита от информационного воздействия на технические средства обработки.
33. Защита от информационного воздействия на общество.
34. Защита от информационного воздействия на психику человека.
35. Применение криптографии.

4. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗЧЕНИЮ ТЕОРЕТИЧЕСКОГО МАТЕРИАЛА

Самостоятельная работа студента начинается с внимательного ознакомления с содержанием учебного курса.

Изучение каждой темы следует начинать с внимательного ознакомления с набором вопросов. Они ориентируют студента, показывают, что он должен знать по данной теме. Вопросы темы как бы накладываются на соответствующую главу избранного учебника или учебного пособия. В итоге должно быть ясным, какие вопросы темы учебного курса и с какой глубиной раскрыты в конкретном учебном материале, а какие вообще опущены. Требуется творческое отношение и к самому содержанию дисциплины.

Вопросы, составляющие ее содержание, обладают разной степенью важности. Есть вопросы, выполняющие функцию логической связки содержания темы и всего курса, имеются вопросы описательного или разъяснительного характера, а также исторического экскурса в область изучаемой дисциплины. Все эти вопросы не составляют сути понятийного, концептуального содержания темы, но необходимы для целостного восприятия изучаемых проблем.

Изучаемая дисциплина имеет свой категориально-понятийный аппарат. Научные понятия — это та база, на которой строится каждая наука. Понятия — узловые, опорные пункты как научного, так и учебного познания, логические ступени движения в учебе от простого к сложному, от явления к сущности. Без ясного понимания понятий учеба крайне затрудняется, а содержание приобретенных знаний становится тусклым, расплывчатым.

Студент должен понимать, что самостоятельное овладение знаниями является главным, определяющим. Высшая школа создает для этого необходимые условия, помогает будущему высококвалифицированному специалисту овладеть технологией самостоятельного производства знаний.

В самостоятельной работе студентам приходится использовать литературу различных видов: первоисточники, монографии, научные сборники, хрестоматии, учебники, учебные пособия, журналы и др. Изучение курса

предполагает знакомство студентов с большим объемом научной и учебной литературы, что, в свою очередь, порождает необходимость выработки у них рационально-критического подхода к изучаемым источникам.

Чтобы не «утонуть» в огромном объеме рекомендованных ему для изучения источников, студент, прежде всего, должен научиться правильно их читать. Правильное чтение рекомендованных источников предполагает следование нескольким несложным, но весьма полезным правилам.

Предварительный просмотр книги включает ознакомление с титульным листом книги, аннотацией, предисловием, оглавлением. При ознакомлении с оглавлением необходимо выделить разделы, главы, параграфы, представляющие для вас интерес, бегло их просмотреть, найти места, относящиеся к теме (абзацы, страницы, параграфы), и познакомиться с ними в общих чертах.

Научные издания сопровождаются различными вспомогательными материалами — научным аппаратом, поэтому важно знать, из каких основных элементов он состоит, каковы его функции.

Знакомство с книгой лучше всего начинать с изучения аннотации — краткой характеристики книги, раскрывающей ее содержание, идейную, тематическую и жанровую направленность, сведения об авторе, назначение и другие особенности. Аннотация помогает составить предварительное мнение о книге.

Глубже понять содержание книги позволяют вступительная статья, в которой дается оценка содержания книги, затрагиваемой в ней проблематики, содержится информация о жизненной и творческой биографии автора, высказываются полемические замечания, разъясняются отдельные положения книги, даются комментарии и т.д. Вот почему знакомство с вступительной статьей представляется очень важным: оно помогает студенту сориентироваться в тексте работы, обратить внимание на ее наиболее ценные и важные разделы.

Той же цели содействует знакомство с оглавлением, предисловием, послесловием. Весьма полезными элементами научного аппарата являются сноски, комментарии, таблицы, графики, списки литературы. Они не только иллюстрируют отдельные положения книги или статьи, но и сами по себе являются дополнительным источником информации для читателя.

Если читателя заинтересовала какая-то высказанная автором мысль, не нашедшая подробного освещения в данном источнике, он может обратиться к тексту источника, упоминаемого в сноске, либо к источнику, который он может найти в списке литературы, рекомендованной автором для самостоятельного изучения.

Существует несколько форм ведения записей:

— план (простой и развернутый) — наиболее краткая форма записи прочитанного, представляющая собой перечень вопросов, рассматриваемых в книге или статье. Развернутый план представляет собой более подробную за-

пись прочитанного, с детализацией отдельных положений и выводов, с выпиской цитат, статистических данных и т.д. Развернутый план — неоценимый помощник при выступлении с докладом на конкретную тему на семинаре, конференции;

— тезисы — кратко сформулированные положения, основные положения книги, статьи. Как правило, тезисы составляются после предварительного знакомства с текстом источника, при его повторном прочтении. Они помогают запомнить и систематизировать информацию.

Составление конспектов

Большую роль в усвоении и повторении пройденного материала играет хороший конспект, содержащий основные идеи прочитанного в учебнике и услышанного в лекции. Конспект — это, по существу, набросок, развернутый план связного рассказа по основным вопросам темы.

В какой-то мере конспект рассчитан (в зависимости от индивидуальных особенностей студента) не только на интеллектуальную и эмоциональную, но и на зрительную память, причем текст конспекта нередко ассоциируется еще и с текстом учебника или записью лекции. Поэтому легче запоминается содержание конспектов, написанных разборчиво, с подчеркиванием или выделением разрядкой ключевых слов и фраз.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Перечень основной литературы:

1. Влацкая И.В., Заельская Н.А., Надточий Н.С. Проектирование и реализация прикладного программного обеспечения / Учебное пособие.- Оренбург: Оренбургский государственный университет, 2015, http://www.iprbookshop.ru/54145.html

2. Карташевский В.Г., Лихтциндер Б.Я., Киреева Н.В., Буранова М.А. Компьютерные сети/ Учебник.- Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016, http://www.iprbookshop.ru/71846.html

Перечень дополнительной литературы:

1. Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия / Учебное пособие.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, http://www.iprbookshop.ru/52217

2. Басалова Г.В. Основы криптографии / Учебное пособие.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, http://www.iprbookshop.ru/52158

3. Скрипник Д.А. Обеспечение безопасности персональных данных / учебное пособие.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, режим доступа http://www.iprbookshop.ru/52153

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. «Университетская библиотека онлайн» - http://biblioclub.ru
2. «Электронно-библиотечная система IPRbooks» http://www.iprbookshop.ru

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На семинарских и практических занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

1	https://www.consultant.ru/ Консультатнт плюс - информационно-правовая система