Содержание

ВВЕДЕНИЕ

Актуальность исследования

В настоящее время проблема защиты информации в целом и проблема защищенности автоматизированных систем как частный случай набирает все большую значимость. Мировое сообщество уже перешло на электронный документооборот, электронные деньги. Все большую популярность набирают электронные системы оплаты услуг, использование электронной почты, IP-телефония. Широкое распространение получили сервисы обмена информацией, мультимедийным контентом, новостями, среди которых наибольшую огласку получили социальные информационные сети. В связи с этим следует выделить такой тип атаки на АС, как «анализ сетевого трафика», которые очень часто применяются злоумышленниками для перехвата паролей, имен учетных записей, номеров банковских счетов[7, 15, 63, 103, 104].

При этом ущерб, нанесенный жертве, зависит от тех действий, которые производились во время сессии. Если в чужие руки попадает информация по кредитным картам, последствия могут оказаться весьма серьезными. Реквизиты этих карт злоумышленники используют для оплаты товаров и услуг по всему миру, естественно, за счет жертвы. Это продолжается до тех пор, пока пострадавший не обнаруживает пропажу денег со счета, что, как правило, происходит лишь в конце месяца, когда он получает выписку по счету[2, 36, 62].

Если злоумышленник получает доступ к корпоративномуэлектронному адресу, то потенциальный ущерб возрастает во много раз. Потери от кражи финансовой информации бывает не просто трудно подсчитать, в некоторых случаях уходят годы на то, чтобы полностью оценить весь причиненный ущерб. Если в результате атаки была украдена и предана огласке конфиденциальная информация (отчеты компании, техническая документация, клиентская база), репутации компании может быть нанесен сокрушительный удар – потеря доверия со стороны клиентов и партнеров, резкое сокращение сбыта продукции компании и даже крах бизнеса [2, 10, 24].

Как видно из статистики, публикуемой различными информационными порталами, число атак на пользовательские данные стремительно растет. При этом особенно уязвимыми элементами сети являются пользователи, использующие беспроводные системы связи [103, 104].

Компания StatCounter отмечает, что с января 2011 года доля мобильного интернет-трафика в среднем по миру выросла почти вдвое с 4,3 до 8,5 процента, при этом двукратный рост мобильного трафика наблюдается ежегодно с 2009 года. В России, по данным StatCounter, доля мобильного трафика в феврале 2012 года составила 2,95% [102].

Наиболее распространенными технологиями мобильной связи являются GSM (европейского стандарта сотовой связи второго поколения) и 3G (от англ. thirdgeneration– третье поколение)[60].

Мобильная связь третьего поколения (3G) строится на основе пакетной передачи данных и обеспечивает более высокую скорость передачи данных, что обуславливает ее широкое распространение среди пользователей Интернет[29, 101].

Как свидетельствует мировая статистика, уровень потерь операторов мобильной связи от разного рода мошенничества и вредительства составляет 2 – 6% от общего объема трафика, а по данным самих компаний он может доходить до 25%. Причем атаки мошенников направлены как против операторов, так и против абонентов [16, 25, 102].

Подсчитано, что из-за мошенничества отрасль мобильной связи во всем мире теряет ежегодно около 25 млрд. долларов, по информации от МГТС (Московской городской телефонной сети) ущерб только по Москве оценивается в пределах 3 – 5 млн. руб. в месяц[104]. Ежегодные убытки операторов сотовой связи в Великобритании, Испании, Германии исчисляются миллионами евро [102]. Поэтому вопросы обеспечения безопасности информации в мобильных сетях являются в настоящее время весьма актуальными и требуют к себе постоянного внимания и анализа.

Не меньшее распространение получили сети Wi-Fi. Большинство современных мобильных устройств оснащаются Wi-Fiадаптерами, а бесплатные точки доступа

покрывают значительную часть территории в крупных городах по всему миру[102]. В феврале 2012г. в Воронеже расположено, по меньшей мере, 70 бесплатных точек доступа[100]. Многие пользователи приобретают устройства для организации беспроводного доступа в своем доме.

Наибольшую опасность для пользователей Wi-Fi представляет возможность перехвата трафика злоумышленником. Чтобы предотвратить нарушение конфиденциальности информации, передаваемой по беспроводному каналу, современные устройства Wi-Fi поддерживают различные протоколы шифрования: WEP, WPA, WPA2 [26, 38, 101]. Однако, как показывает статистика, полученная Лабораторией Касперского, большинство администраторов не используют шифрование пакетов, либо используют наиболее уязвимый для криптоанализа алгоритм WEP. Наиболее защищенный протокол WPA2 используется в единичных случаях [104].

Многие программные анализаторы сетевых пакетов (снифферы) имеют также функции дешифровки информации, зашифрованной с помощью протокола SSL [104]. Это значит, что нельзя гарантировать безопасность даже так называемых безопасных соединений с регистрационными страницами. В зависимости от степени шифрования трафика киберпреступникам может потребоваться больше или меньше усилий на его расшифровку – усилий, которые они прилагают, пока успокоенные ложным чувством безопасности жертвы производят банковские операции онлайн или проверяют свою почту[29, 104].

Таким образом, большинство пользователей, использующих публичные точки доступа, не подозревают о том, что их конфиденциальная информацияможе легко попасть в руки злоумышленника. Что касается тех, кто использует точки доступа для беспроводного подключения к домашней сети, то помимо потери регистрационных данных и паролей существует риск использования злоумышленником его домашнего подключения к сети, которое пользователь добросовестно оплачивает у своего провайдера в соответствии с тарифным планом[102, 103, 104].

Из выше сказанного очевидно, что атаки типа «анализ сетевого трафика»требуют глубокого анализа, изучения способов реализации, а также разработки специфических средств и методов создания системы защиты.

Степень научной разработанности

Как показывает анализ известной литературы, моделирование атак типа «анализ сетевого трафика»на беспроводные каналы связи ранее не проводился, что не позволяет обосновать требования к системе защиты АС от этих атак.

Таким образом, исходя из актуальности и степени научной разработанности проблемы защищенности АС от атак типа «анализ сетевого трафика», представляется целесообразным проведение исследований в данном направлении, изучение алгоритмов реализации атак с последующей разработкой мер по их противодействию.

Объектом исследования являются автоматизированные системы, имеющие в своем составе компоненты, осуществляющие передачу информации по беспроводным каналам, функционирующие в условиях высокого риска реализации атак типа «анализ сетевого трафика».

Предметом исследования выступают процессы реализации атак типа «анализ сетевого трафика» на беспроводные каналыАС и методы противодействия им.

Цель и задачи исследования

Целью настоящей работы является управлениериском от реализации атаки типа «анализ сетевого трафика» на беспроводные каналы АСс целью обеспечения защищенности этих систем.

Для достижения данной цели необходимо решить следующие задачи:

1. Разработать модель атаки типа «анализ сетевого трафика» с учетом особенностей построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

2. Разработатьриск-модельреализации атак типа «анализ сетевого трафика» на основе анализапостроенной модели атаки, учитывающую особенности построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

3. Исследовать динамическую риск-модельреализации атак типа «анализ сетевого трафика» на АС, включающую в себя множество компонентов, участвующих в процессе передачи информации по беспроводным каналам.

4. Разработать новый подход к управлению рискомреализации атак типа «анализ сетевого трафика» на АС, включающую в себя множество компонентов, участвующих в процессе передачи информации по беспроводным каналам.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

Методы исследования

Для решения поставленных задач необходимо использовать методы системного анализа,математической статистики, теории риска, теории вероятности и информационно-логического метода, предусматривающего анализ большого количества информационных источников и справочной литературы.

На защиту выносятся следующие основные положения работы:

1. Модель реализации атак типа «анализ сетевого трафика» с учетом особенностей построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

2. Риск-модель реализации атак типа «анализ сетевого трафика» на основе анализа построенной модели атаки, учитывающей особенностей построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

3. Результаты исследования динамической риск-моделиреализации атак типа «анализ сетевого трафика» на АС, включающей в себя множество компонентов, участвующих в процессе передачи информации по беспроводным каналам..

4. Алгоритм подхода к управлению рискомреализации атак типа «анализ сетевого трафика» на АС, включающей в себя множество компонентов, участвующих в процессе передачи информации по беспроводным каналам.

Научная новизна исследования

1. В отличие от аналогов, модель реализации атак типа «анализ сетевого трафика»на беспроводные каналы АСучитываетособенности построения ее беспроводных каналов передачи информации, такие как алгоритмы канального кодирования и шифрования данных.

2. В отличие от аналогов, полученная риск-модель атак типа «анализ сетевого трафика» на беспроводные каналы АС содержит более точные значения параметров риска, а также выражения для нахождения диапазонов ущербов по заданному уровню риска.

3. В отличие от аналогичных, исследуемая динамическая риск-модельреализации атак типа «анализ сетевого трафика» включает в себя выражения для экстремумов интегрального риска АС, а так же выражение для смещения интегрального риска в сторону больших значений ущерба

4. Отличительной особенностью подхода к управлению риском реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС является оценка эффективности комплекса мер и средств контроля и управления риском, а также обработка риска информационной безопасности в соответствии с положениями государственных стандартов РФ.

Практическая ценность работы заключается в следующем.

1. Модель реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС позволяет учитывать наиболее опасные каналы в зависимости от приме-

няемых алгоритмов кодирования и шифрования трафика и дает возможность уделить особое внимание защите от этих типов атак.

2. Построенная риск-модель может применяться для оценки рисков реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС, определения диапазона ущербов по заданному уровню риска, а также построения систем, устойчивых к атакам данного типа.

3. Исследуемая динамическая риск-модель включает выражения для интегрального риска АСи его экстремумов, которые позволяют оценить защищенность системы в целом, а также выявить наиболее уязвимые компоненты. Динамическая риск-модель позволяет так же определить оптимальные значения параметров компонент АС, при которых максимальное значение интегрального риска и диапазона ущербов по заданному уровню риска не превышают требуемого значения.

4. Подход к управлению риска реализации атак может применяться для оценки эффективности применяемых мер и средств контроля и управления рискомреализации атак типа «анализ сетевого трафика» на беспроводные каналы АС и выбора наиболее подходящих комплексов мер и средствс целью получения приемлемых показателей риска информационной безопасности АС, подвергающихся атакам типа «анализ сетевого трафика» на беспроводные каналы передачи информации.

ЗАКЛЮЧЕНИЕ

Работа посвящена исследованию рисков реализации атак типа «анализ сетевого трафика» на АС, имеющие в своем составе элементы, осуществляющие передачу информации по беспроводным каналам.

В ходе ее выполнения были получены следующие результаты:

1. На основании выполненных исследований разработана научная идея, обогащающая концепцию регулирования интегрального риска реализации асинхронных атак в АС путем выражения смещения интегрального риска через первоначальное выражение функции интегрального риска системы.

2. Предложеныоригинальные суждения по оценке интегрального риска АС, включающей несколько компонент, осуществляющих передачу информации по беспроводным каналам, и экстремумов рискав рамках регулирования риска реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС.

3. Возможностью применения исследуемой динамической риск-модели для оценки рисков реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС доказана перспективность и состоятельность использования полученных выражений для экстремумов интегрального риска с целью его анализа в АС, выявления уязвимых компонент, защите которых необходимо уделить особое внимание, а также для построения защищенных АС.

4. Изменена трактовка понятия анализа сетевого трафика с точки зрения реализации перехвата трафика, циркулирующего в АС, технологического усовершенствования и возможности реализации перехвата в беспроводных каналах АС, а также учитывающая особенности построения таких каналов, такие как наличие канального кодирования и шифрования данных.

5. В ходе проведения оценки остаточного риска доказано, что функция рискареализации атак типа «анализ сетевого трафика» на беспроводные каналы АС является распределением с «тяжелым хвостом», что позволяет оценить остаточный риск путем оценки тяжести «хвоста» для данного вида распределения.

6. Применительно к проблематике работы эффективно, с получением обладающих новизной результатов, использован комплекс базовых методов исследования, таких как метод системного анализа, теории риска, теории вероятности, математической статистики.

7. В работе изложены положения государственных стандартов РФ, таких как ГОСТ Р ИСО/МЭК 27005-2010, ГОСТ Р ИСО/МЭК 17799-2005, на основании которых производилась обработка рискареализации атак типа «анализ сетевого трафика» на беспроводные каналы АС.

8. В ходе исследования динамический риск-модели реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС была выявлена проблема поиска минимумов суммарного риска, заключающаяся в отсутствии закономерности расположения минимумов суммарного риска относительно пиков риска отдельных компонент и пиков суммарного риска АС.

9. Изучен генезис процесса реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС, с учетом качественных особенностей и технологического развития технологий беспроводной передачи информации, а также объектов, на которые они направлены, кроме того, учитывались факторы, влияющие на этот процесс.

10. В ходе исследования динамический риск-модели реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС осуществлено обобщение полученного решения для АС, состоящей из двух компонент, на случай, при котором система состоит из нескольких компонент, осуществляющих передачу информации по беспроводным каналам.

11. Основные теоретические положения работы обсуждались на межрегиональной научно-практической конференции «Инновации и информационные риски».

12. Полученные результаты исследований имеют практическое применение для исследования защищенности АС, имеющих в своем составе компоненты, осуществляющие передачу информации по беспроводным каналам, наступление ущерба которых имеет распределение хи-квадрат.

13. В работе представлены предложения по дальнейшему совершенствованию и разработке новых методов регулирования риска реализации атаки типа «анализ сетевого трафика» на беспроводные каналы АС, позволяющие создать более эффективные и универсальные методики управления.

14. Оценка достоверности результатов исследования основана на анализе статистических данных реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС в период с 01.01.2011 по 31.12.2011, предоставленных отделением министерства США, занимающимся экономическими преступлениями.

15. Идея проводимых исследований базируется на обобщении полученных ранее результатов исследования и оценки риска реализации атаки типа «анализ сетевого трафика» на беспроводные каналы АС, а также на применение положений государственных стандартов для разработки методики обработки рисков реализациииатак типа «анализ сетевого трафика» на беспроводные каналы АС.

16. При проведении исследований было использовано сравнение результатов исследования, полученных ранее по рассматриваемой тематике. В исследовании не проводилось регулирование рисков, поэтому в авторской работе применялась динамическая риск-модель, позволяющая разработать эффективные подходы к управлению рисками реализации атаки типа «анализ сетевого трафика» на беспроводные каналы АС.

17. В работе использованы результаты применения современных систем сбора и обработки исходной информации, в частности, – статистических данных. Применялись методы их анализа и предварительной обработки.

18. Личный вклад состоит в участии на всех этапах процесса исследования, непосредственном участии в получении исходных данных, участии в апробации результатов исследования, подготовке основных публикаций по выполненной работе.

СПИСОК ЛИТЕРАТУРЫ

1 Альгин А.П. Риск и его роль в общественной жизни. – М.: Мысль, 1989. – 378 с.

2 Балакирский В.Б. Безопасность электронных платежей // Конфидент. 1996, № 5, С. 47-53.

3 Балдин К.В. Управление рисками: Учеб. пособие / К.В. Балдин, С.Н. Воробьев. – М.: Юнити-Дана, 2005. – 511с.

4 Баранов А. П. и др. Математические основы информационной безопасности. Орел: ВИПС, 1997, С. 50.

5 Барсуков В.С., Водолазский В.В. Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей. М.: Электронные знания, 1993. – 300 с.

6 Бейнар И.А. Формирование затрат на информационную безопасность//Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2009. Вып. 1. С.117-120.

7 Белоусов И.В. Информационная безопасность телекоммуникационных сетей: проблемы и пути их решения // Безопасность информационных технологий. – М.: Альфа, 1999, № 1. – 54 с.

8 Богирев В.Г., Гончаров В.В., Серов Р.Е.Основы современной криптографии. - М.: «Горячая линия – Телеком», 2001. – 165 с.

9 Большаков А.А., Петряев А.Б., Платонов В.В., Ухлинов Л.М. Основы обеспечения безопасности данных в компьютерных системах и сетях. Ч. 1. Методы, средства и механизмы защиты данных. – СПб.: Конфидент, 1996. – 400 с.

10 Борисов В.И., Радько Н.М., Скобелев И.О., Науменко Ю.С. Оценка рисков информационно-телекоммуникационных систем, подвергающихся НСД-атакам//Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2011. Вып. 1. С. 5-24.

11 Борисов В.И., Щербаков В.Б., Ермаков С.А. Спектр уязвимостей беспроводных сетей стандарта IEEE802.11 //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2008. Вып. 3. С. 431-434.

12 Введение в криптографию. BYTE/Россия. № 12, 1999. С. 18-25. (Перевод В. Казеннова статьи Дж Чанддера «Cryptography 101»).

13 Венцель Е.С. Теория вероятности – 1969 г. – 564 с.

14 Вероятность и математическая статистика: энциклопедия // Гл. ред. акад. РАН Ю.В. Прохоров. – М.: Большая Российская энциклопедия, 1999. – 910 с.

15 Владимиров И.В., Асеев В.Н.Информационная безопасность телекоммуникационных систем: Учеб. пособие. – Воронеж: Воронеж. гос. техн. ун-т, 2005. – 78 с.

16 Володин А.В., Устинов Г.Н., Алгулиев Р.М. Как обеспечить безопасность сети передачи данных // Технологии и средства связи, 1999, №4, С. 33-35.

17 Галатенко В. А. Стандарты информационной безопасности. Издательство: Интернет-университет информационных технологий, 2006 г.

18 Галатенко В. Информационная безопасность – основы. 1996, № 1, с.6-28.

19 Герик Т. Информационная база для оценки риска / Т. Герик // LAN: журнал сетевых решений. – М.: Единая Европа, 2006. – №9. – С. 22-25.

20 Гончаренко Л.П. Риск-менеджмент: учебное пособие / Под ред. д-ра тех. наук. проф., засл. деятеля науки РФ Е.А. Олейникова; Л.П. Гончаренко, С.А. Филин. – М.: Кнорус, 2006. – 216 с.

21 Горявский Ю. Криптография для сетей. BYTE/Россия. № 1, 1999. (Обзор криптографических алгоритмов), С. 36-38.

22 ГОСТ Р ИСО/МЭК 27005-2010 – Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

23 ГОСТ Р ИСО/МЭК 17799-2005– Информационная технология. Практические правила управления информационной безопасностью.

24 Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения / В.М. Гранатуров – М.: Издательство "Дело и Сервис", 2002. – 160 с.

25 Давыдовский А.И., Дорошкевич П.В. Защита информации в вычислительных сетях // Зарубежная радиоэлектроника. 1989. № 12. С. 60-70.

26 Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. Издательство: ТИД "ДС". 2008 г. 688 с.

27 Доронин А. Экономическая и информационная безопасность. Тула, 1997, С. 122.

28 Ефремов А. Сетевые атаки и средства борьбы с ними // Computer Weekly № 14, 1998, С. 14-17.

29 Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. СПб.: Изд. СпбУ, 1999,С.60-63.

30 Зубов А. Ю. Криптографические методы защиты информации. – М.: Гелиос АРВ, 2005. – 192 с.

31 Иванов В. П. Математическая оценка защищенности информации от несанкционированного доступа // Специальная техника. 2004, N 1. С. 58 –64.

32 Информационная безопасность. Information Security. Издательство: Оружие и технологии России, 2009 г. 256 с.

33 Касперски Крис. Техника и философия хакерских атак. – Издательство СОЛОН-Р, 2004. – 272 с.

34 Кристиан Барнс, Тони Боутс, Дональд Ллойд и др. Защита от хакеров беспроводных сетей. – Издательство ДМК Пресс, 2005. – 480 с.

35 Комов С.А., Ракитин В.В. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-Траст, 2009. - 304 с.

36 Конахович Г.Ф. Защита информации в телекоммуникационных системах. – М.: МК-Пресс, 2005. –288 с.

37 Кобзарь М., Долинин М. Общие критерии оценки безопасности информационных технологий. Версия 2.0. Что нового?/Jet Info. Информационный бюллетень. 1998. № 5-6.

38 Кристиан Барнс, Тони Боутс, Дональд Ллойд, Эрик Уле, Джеффри Посланс, Дэвид М. Зенджан, Нил О'Фаррел. Защита от хакеров беспроводных сетей.

Hack Proofing Your Wireless Network. Издательства: Компания АйТи, ДМК пресс, 2005 г. 480 с.

39 Куканова Н. Методы и средства анализа рисков и управление ими в ИС // Byte/Россия. 2005. № 12. С. 69–73.

40 Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Курс лекций. Учебное пособие. Издательство: Интернет-университет информационных технологий, 2005 г. 608 с.

41 Левин М. Хакинг и фрикинг: методы, атаки, секреты, взлом и защита. М.: Оверлей. 2000, 416с.

42 Леннон Э.. Компьютерные атаки: что это такое и как с этим бороться. BYTE/Россия. № 2, 2000. С.51-54. Бюллетень лаборатории информационных технологий NIST, май 1999 г.

43 Леонтьев Б. Хакеры и Интернет. М., 1998 г.

44 Леонтьев Б. Хакеры, взломщики и другие информационные убийцы. М.: Познавательная книга, 1999 г.

45 Лукацкий А.В. Адаптивная безопасность сети//КомпьютерПресс. 1999. № 8.

46 Лукацкий А.В. Атаки на информационные системы. «Электроника. Наука. Технологии и Бизнес». 2000, № 1, с.42-44.

47 Лукацкий А.В. Обнаружение атак – СПб.: БХВ-Петербург, 2001. – 624 с.

48 Лукацкий А.В. Обнаружение атак в новом тысячелетии//PCWeelc/RE. 1999. № 33

49 Лукацкий А.В. Комплексный подход к обеспечению информационной безопасности. – Системы безопасности, связи и телекоммуникаций. 1998. – №1. – 50 с.

50 Лукацкий А.В. Новые грани обнаружения и отражения угроз. Системы безопасности, связи и телекоммуникаций. 2000. №36.

51 Медведовский И., Семьянов П., Платонов В. Атака через Интернет.Под ред. П.Д. Зегжды. СПб.: Мир и семья, 1997.– 200с.

52 Мерритт Максим, Дэвид Поллино. Безопасность беспроводных сетей. Wireless Security. Издательства: ДМК пресс, Компания АйТи, 2004 г. 288 с.

53 Найк Д. Стандарты и протоколы Интернета / Пер. с англ. М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd», 1999, С. 156.

54 Онтанъон Рамон Дж. Какова реальная угроза хакеров вашей сети?//LAN/Журнал сетевых решений. 2000. № 3.

55 Онтанъон Рамон Дж. Создание эффективной системы выявления атак//LAN/Журнал сетевых решений. 2000. № 10.

56 Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В., Гончаров И.В., Маслихов П.А., Мешкова Е.А., Морозова Н.М., Рязанов С.В., Субботина Е.В., Транин В.А. Риски распределенных систем: методики и алгоритмы, оценки и управление. //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2010. Вып. 4. С. 485-531.

57 Остапенко О.А. Риски систем: оценка и управление: учеб. пособие // О.А. Остапенко, Д.О. Карпеев, В.Н. Асеев; под ред. Ю.Н. Лаврухина. – Воронеж: ГОУВПО «ВГТУ», 2006. – 247 с.

58 Перин В.А. Генерация, распределение и использование криптографических ключей. Защита информации. 1992, № 1, С. 157-184.

59 Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. Издательство: Академия, 2006 г. 240 с.

60 Попов В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности. Издательство: Финансы и статистика, 2005 г.. 176 с.

61 Радько Н.М., Скобелев И.О. Аналитическое моделирование процессов реализации удаленных атак при помощи аппарата теории сетей Петри-Маркова: сниффинг пакетов в сети без коммутаторов //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2008. Вып. 4. С. 585-588.

62 Радько Н.М., Скобелев И.О. Аналитическое моделирование процессовреализации удаленных атак типа "сканирование сети" //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2009. Вып. 1. С. 133-134.

63 Радько Н.М., Скобелев И.О. Концептуальные основы риск-анализа и оценки эффективности защиты информационно-телекоммуникационных систем от атак несанкционированного доступа //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2011. Вып. 2. С. 239-244.

64 Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа.—М: Радио Софт, 2010—232 с.

65 Романец Ю.В., Тимофеев П.А., Щаньгин В.Ф. Защита информации в компьютерных системах и сетях – М.: Радио и связь, 2001. – 300 с.

66 Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

67 Семенов Ю. А. Алгоритмы телекоммуникационных сетей. В 3 частях.

68 Семкин С.Н. Защита информации. Часть 1. Основы информационной безопасности объектов информационно-телекоммуникационной системы. Курс лекций. Орел: ВИПС, 2000. 269 с.

69 Сердюк В. Системы обнаружения компьютерных атак и их роль в защите информационных сетей. BYTE/Россия. 2000 № 10.

70 Симонов С. Анализ рисков, управление рисками. Jet Info. Информационный бюллетень. № 1(68), 1999, С. 2-28.

71 Скобелев И.О. Оценка эффективности защиты информационно-телекоммуникационной системы на основе построения риск-модели системы, функционирующей в условиях реализации атак, связанных с удаленным доступом //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2010. Вып. 4. С. 603-606.

72 Степанов Е.А. Безопасность информационных ресурсов // Делопроизводство. 1998, №2, С. 20-22.

73 Томилин В. Виды сетевых атак. BYTE/Россия. № 11. 2000,С.68-73.

74 Хелд Г. Технологии передачи данных. – Издательство Питер, 2003. – 720 с.

75 Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002 г.

76 Шахнович И. Современные технологии беспроводной связи. – М.: Техносфера, 2004. – 168 с.

77 Шипли Г. Анатомия сетевого вторжения. Сети и системы связи. 2000. №1.

78 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - М.:Наука и техника, 2002 г.

79 Щербаков В.Б. Классификация беспроводных сетей по набору применяемых средств защиты //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2009. Вып. 1. С. 125-128.

80 Щербаков В.Б., Ермаков С.А. Особенности риск-оценки безопасности беспроводных сетей //Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2009. Вып. 1. С. 135-136.

81 Щербаков В.Б., Ермаков С.А. Атаки на беспроводные сети стандарта IEEE802.11 с использованием уязвимостей системы аутентификации // Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2008. Вып. 2. С. 298-299.

82 Язов Ю.К. Проектирование систем защиты информации в информационно-телекоммуникационных системах: Учеб. пособие.– Воронеж: Воронеж. гос. техн. ун-т, 2004. – 143 с.

83 Advances in cryptology: Proceedings of Eurocrypt'94. Berlin, 1995.

84 Basic Cryptanalysis. US Army field manual № 34-40-2, 1990.

85 Barabasi A-L. Scalefree characteristics of random networks: the topology of the World Wide Web / A-L Barabasi, H. Jeong . – Physica A 281, 2000.

86 Burrows M., Abadi M., Needham R. A Logic of Authentication // Proc. Royal Society.Series A.1989.Vol. 426,№> 1871.P.233-271.

87 Diffie W., van Oorschot P.C., Wiener M.J. Authentication and Authenticated Key Exchanges // Designs, Codes and Cryptography, v. 2, 1992, P. 107-125.

88 ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, V. IT-31, 1985г.

89 Feistel H. Cryptography and computer privacy // Scientific American. 1973. Vol. 228. №5.

90 Guide to BS7799 risk assessment and risk management. DISC PD 3002, 1998. Методический материал Британского института стандартов BSI.

91 Information security management: an introduction. DISCPD 3000, 1998. Методический материал Британского института стандартов BSI

92 Hill, B. A simple general approach to inference about the tail of a distribution // Ann . Statist. 1975. N 3.

93 J. C. Grauenthal. Mathematical Modeling in Epidemiology / C. Grauenthal. – Springer-Verlag, New York, 1980.

94 Kent S.T. Internet Security Standards: Past, Present and Future // StandardView. 1994. Vol. 2, № 2. P.78-85.

95 Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Lecture Notes in Computer Science. 1996.Vol. 1109. Kumar Sandeep. Classification and detection of computer intrusions//Purdue University, 1996

96 Leskovec J. Cost-effective outbreak detection in networks / J. Leskovec, A. Krause, C. Guestrin, C. Faloutsos, J. VanBriesen, N. Glance // In 13th ACM SIGKDD International conferences on Knowledge Discovery and Data Mining, 2007.

97 Odlyzko A.M. Public Key Cryptography // AT&T Technical Journal. Sept./Oct. 1994. P. 17-23.

98 Pierson L.G., Witzke E. L. A Security methodology for computing networks // AT&T TECHNICAL Journal. 1988, May-June.

99 Schneier B. Applied Cryptography. John Wiley & Sons, be., 1996.

100 2ГИС – электронный справочник г. Воронежа – Электрон. дан. – Режим доступа: http://voronezh.2gis.ru

101 Википедия – свободная энциклопедия – Электрон. дан. – Режим доступа: http://ru.wikipedia.org.

102 Информационный новостной портал. – Электрон. дан. – Режим доступа: http://www.lenta.ru.

103 Информационный портал по безопасности SecurityLab.ru.- Электрон. дан. – Режим доступа: http://www.securitylab.ru.

104 Портал по безопасности Лаборатории Касперского.- Электрон. дан. – Режим доступа: http://www.securelist.com/ru.

105 Kismet – описание продукта. – Электрон. дан. – Режим доступа: http://www.kismetwireless.net/documentation.shtml

106 WinPcap – официальный сайт. – Электрон. дан. – Режим доступа: http://www.winpcap.org

107 Wireshark –официальный сайт. – Электрон. дан. – Режим доступа: http://www.wireshark.org

8 (952) 106-88-60 vk.com/a.projectit a.projectit