МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Разработка регламента защищенности к проектируемым информационным системам

Методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03

Курск 2022

УДК 004.056.55

Составители: О.А. Демченко

Рецензент

Кандидат технических наук, доцент *А.Л. Марухленко*

Разработка регламента защищенности к проектируемым информационным системам: методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т; сост. О.А. Демченко Курск, 2022. - 14 с.

Содержат сведения по вопросам информационной безопасности. Указывается порядок выполнения лабораторной работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания разработаны для изучения дисциплин, связанными с безопасностью эксплуатации телекоммуникационных систем.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл.печ. л._____ . Уч.-изд.л _____. Тираж 30 экз. Заказ_____.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1. Краткие теоретические сведения

Защита информации является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и осуществляется в соответствии с установленным руководящими документами порядком в виде системы (подсистемы) защиты информации.

Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в автоматизированной системе.

Защита конфиденциальной информации осуществляется на основании федеральных законов «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», Указа Президента Российской Федерации от 06.03.1997 г. № 188 «Перечень сведений конфиденциального характера», «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 09.09.2000 г. № Пр.-1895, других нормативных правовых актов по защите информации, а также опыта реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

В качестве примера рассмотрим одну из наиболее важных задач, решаемых в области защиты информации, – обеспечение безопасности персональных данных граждан.

Для того чтобы ее решить, необходимо не только придерживаться порядка, установленного нормативными и методическими документами, но и хорошо ориентироваться в том, что касается классификации информационных систем и категорий персональных данных, применяемых технологий и средств защиты.

Основным законодательным актом в области защиты персональных данных является Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г. Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой органами государственной власти, иными государственными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

В соответствии с законом «О персональных данных» уполномоченные органы с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливают:

— уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

— требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

— требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Уровень защищённости персональных данных определяется на этапе классификации информационной системы персональных данных в соответствии с Постановлением Правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г.

Устанавливаются 4 уровня защищённости персональных данных в зависимости от категории данных, количества субъектов персональных данных и типа угроз безопасности персональных данных, актуальных для системы. К каждому из четырех уровней предъявляются общие требования к защите данных.

Формирование конкретных требований к системе защиты информации (персональных данных) осуществляют в соответствии с приказом ФСТЭК № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных описаны в Постановлении Правительства № 512 от 06.07.2008 г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Требования к процессу обработки персональных данных, осуществляемому без использования средств автоматизации, установлены Постановлением Правительства № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г.

Все описанные выше законодательные акты и нормативные документы в области защиты персональных данных содержат описание организационных и технических мер обеспечения безопасности персональных данных за исключением требований, предъявляемых в случае использования криптографических (шифровальных) средств.

В случае применения криптографических средств защиты информации, их разработка, внедрение и эксплуатация осуществляется в соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденными приказом ФСБ № 149/54-144 от 21.02.2008 г., а также в соответствии с «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными приказом ФСБ № 149/6/6-622 от 21.02.2008 г.

При построении модели угроз и модели вероятного нарушителя безопасности информации (персональных данных) применяют «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», а также «Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Для учреждений здравоохранения, социальной сферы, труда и занятости составлен документ «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости».

Таким образом, каждый из этапов построения комплексной системы защиты информации регламентируется определенными законодательными и нормативными актами Правительства РФ, ФСТЭК и ФСБ, определяющими порядок и методику создания системы защиты информации, требования к

ней, а также содержание организационных и технических мер по обеспечению безопасности информации.

Состав нормативно-методического обеспечения КСЗИ определяют:

– законодательные акты – законы, указы президента, постановления правительства, кодексы (гражданский, уголовный, административный), ГОСТы;

– руководящие методические документы – документы министерств и ведомств (Гостехкомиссия, ФСБ), а также документы, разработанные на предприятиях по вопросам ЗИ;

– информационно-справочная база – словари, каталоги, специализированные журналы, справочники, электронные БД.

Нормативные документы, определяющие правила безопасности должны удовлетворять следующим требованиям:

– соответствовать структуре, целям и задачам ИС;

– описывать общую программу обеспечения безопасности сети, включая вопросы эксплуатации и усовершенствования;

– перечислять возможные угрозы информации и каналы утечки;

– перечислять рекомендуемые защитные меры;

– определять ответственных за внедрение и эксплуатацию всех средств защиты;

– определять права и обязанности пользователей;

– содержать перечень и классификацию возможных кризисных ситуаций;

– определять порядок разрешения споров в случае возникновения конфликтов.

В комплект внутренних нормативных и методических документов по обеспечению функционирования КСЗИ на предприятии должны входить документы, регламентирующие:

– перечень сведений, подлежащих защите;

– порядок обращения сотрудников с конфиденциальной информацией;

– меры по предотвращению НСД к информационным ресурсам и АС;

– обмен информацией со сторонними организациями;

– пропускной и внутриобъектный режим;

– порядок эксплуатации АС предприятия;

– действия должностных лиц и персонала предприятия в условиях ЧС, обеспечения бесперебойной работы и восстановления;

– планы защиты АС;

– порядок разработки, испытания и сдачи в эксплуатацию ПС;

– порядок закупки программных и аппаратных средств (в том числе средств ЗИ);

– порядок эксплуатации технических средств связи и телекоммуникации

2. Индивидуальное задание студента

Составить перечень мероприятий необходимых для построения КСЗИ с учётом нормативно-методических актов.

Выполнение работы.

В соответствии с вариантом нужно правильно состав шаблон документа на основе нормативно- правовой документации по ИБ. Наименование ИС придумать по желанию. Пример шаблона на основе 1 варианта прилагается.

Вариант	Документ
1	На основе НПА по ИБ составить документ, описывающий перечень сведений, подлежащих защите.
2	На основе НПА по ИБ составить документ, описывающий,

	порядок обращения сотрудников с конфиденциальной информацией.
3	На основе НПА по ИБ описать меры по предотвращению НСД к информационным ресурсам.
4	На основе НПА по ИБ составить инструкцию, описывающую действия должностных лиц и персонала предприятия в условиях ЧС.
5	На основе НПА по ИБ составить инструкцию, описывающую функциональные обязанности администратора безопасности информации на ОИ
6	На основе НПА по ИБ составить документ, описывающий, определение контролируемой зоны, перечня помещений на ОИ.
7	На основе НПА по ИБ составить инструкцию по организации режима обеспечения безопасности помещений на ОИ

3. Пример.

Вариант 1. Возьму за основу. ИС «Бухгалтерия» предприятия ООО «Пластиковые окна».

УТВЕРЖДАЮ

_____ (Ф.И.О. руководителя)

« ____» _____ 202_ г.

Перечень защищаемых информационных ресурсов информационной системы ИС «Бухгалтерия» ООО «Пластиковые окна»

Защищаемыми информационными ресурсами в информационной системе «Бухгалтерия» являются базы данных, содержащие информацию ограниченного доступа, а именно персональные данные граждан, оператором (обладателем) которых является ООО «Пластиковые окна». Перечень баз

данных, средства работы с ними, цель и содержание обработки персональных данных, правовое основание и места обработки представлены в таблице №1.

Состав идентификаторов ПДн, обрабатываемых в каждой из баз данных, представлен в таблице №2.

Таблица №1 — Перечень баз данных, средства работы с ними, цель и содержание обработки персональных данных

№	Наименование базы данных	Программное обеспечение обработки ПДн	Цель обработки ПДн	Правовое основание обработки ПДн
Кабинет №10				
1.	ИС «Бухгалтерия»	1 С	Хранение документов	Федеральный закон РФ от ….

Таблица №2 — Состав идентификаторов персональных данных

№	Перечень идентификаторов персональных данных
ИС «Бухгалтерия»	
Общие сведения:	
1.	Фамилия, имя, отчество
2.	Дата рождения
3.	Реквизиты документа, удостоверяющего личность (тип документа, серия и номер, дата и место выдачи, кем выдан)
4.	Место учебы
5.	…
6.	…

(Должность) Ф.И.О.

4. Контрольные вопросы

1. Каким документом определяются требования к защите персональных данных?
2. Какой документ, регламентирует использование криптографических средств защиты в информационных системах?
3. Назовите перечень документов используемых для защиты персональных данных.
4. Какие документы предоставляет заказчик для проведения испытаний органу по аттестации?
5. Что должен содержать аттестат соответствия?

5. Содержание отчёта

Отчёт обучающегося должен содержать:

— титульный лист,

— цель работы,

— выполнение заданий,

— краткий вывод,

— ответы на контрольные вопросы

6. Библиографический список

1. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов – 3-е изд., стер. – Москва: Академия, 2008. – 331 с.
2. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т.Р. Методы и средства инженерно-технической защиты информации: учебное пособие. 2-е изд., стер. - М.: Флинта, 2011. - 187 с.
3. Чипига А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие – М.: Гелиос АРВ, 2010. – 336 с.
4. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие – Брянск: БГТУ, 2005. – 269 с.
5. Аверченков, В.И. Организационная защита информации: учеб. пособие – Брянск: БГТУ, 2010. – 184 с.
6. ГОСТ Р 51624-00 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
7. ГОСТ Р 51275-99 Защита информации. Объект информатизации, факторы, воздействующие на информацию. Общие положения.
8. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 254 с.
9. Федеральный закон № 149-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
10. Федеральный закон № 152-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
11. Грибунин В.Г., Чудовский В.В. КСЗИ на предприятии. – М.: Академия, 2009. – 416 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Контроль защищенности информационных систем

Методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03

Курск 2022

УДК 004.056.55

Составители: О.А. Демченко

Рецензент

Кандидат технических наук, доцент *А.Л. Марухленко*

Контроль защищенности информационных систем: методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т; сост. О.А. Демченко Курск, 2022. - 9 с.

Содержат сведения по вопросам информационной безопасности. Указывается порядок выполнения лабораторной работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания разработаны для изучения дисциплин, связанными с безопасностью эксплуатации телекоммуникационных систем.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл.печ. л._____ . Уч.-изд.л _____. Тираж 30 экз. Заказ_____.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1. Краткие теоретические сведения

Контроль состояния защиты информации в АС (контроль защищенности АС) осуществляется с целью своевременного выявления и предотвращения несанкционированного доступа к информации, ее утечки по техническим каналам, преднамеренных специальных воздействий на информацию (носители информации) и других угроз информационной безопасности по нормам и методикам, утвержденным ФСТЭК России.

Контроль состояния защиты информации и оценка эффективности средств защиты являются неотъемлемой составной частью работ по защите информации при создании и эксплуатации ИС.

Основными задачами контроля являются:

1. Проверка соответствия принятых и принимаемых мер по защите информации.

2. Проверка своевременности и полноты выполнения требований нормативных документов, регламентирующих организацию и порядок осуществления мероприятий по защите информации.

При проведении контроля защищённости организация подтверждает:

1. Созданная система обеспечивает выполнение требований по защите информации при эксплуатации АС.

2. Меры, средства и мероприятия, проводимые в целях защиты информации, соответствуют предъявляемым к АС требованиям безопасности информации.

3. Средства защиты информации настроены и используются правильно.

4. Рекомендации предшествующих проверок реализованы в полной мере.

Порядок проведения контроля защищённости

Испытания контроля защищенности проводятся в следующем порядке:

1. Составление технического паспорта. Для любых информационных систем, в том числе для ИСПДн и АС, должен составляться технический паспорт, в котором отражается текущее состояние системы. В нем перечисляются модели и серийные номера основных и вспомогательных технических средств и оборудования, входящего в информационную систему.

2. Анализ актуальных угроз безопасности. На данном этапе контроля защищённости производится разбор актуальных для информационной системы угроз с описанием их возможного негативного воздействия на систему и методов защиты, применяемых против них в организации.

3. Анализ средств защиты информации. Данный этап включает в себя обзор СЗИ, применяемых в организации. Особое внимание обращают на соответствие применяемых СЗИ уровню и классу защищённости информационной системы.

4. Контроль целостности ПО. Этап включает в себя проверку целостности всего программного обеспечения, в том числе СЗИ. Для этого определяют состав ПО СЗИ, с помощью прикладного ПО получают контрольные суммы. Полученные результаты контрольных сумм с эталонными.

5. Анализ уязвимости сети. При помощи сетевого сканера сеть информационной системы проверяется на наличие уязвимостей. Обнаруженные уязвимости необходимо представить к устранению.

2. Индивидуальное задание студента

Провести контроль защищенности ИС.

Для проведения контроля защищенности:

1. Проанализировать актуальные угрозы безопасности ИС, обрабатываемых на объекте информатизации.

На данном этапе контроля защищённости производится разбор актуальных для информационной системы угроз с описанием их возможного негативного воздействия на систему и методов защиты, применяемых против них в организации.

2. Для ОИ подобрать СЗИ с учетом актуальных угроз.

Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

3. Контрольные вопросы

1. Что включает в себя типовая методика анализа защищенности ИС предприятия?
2. Какие исходные данные необходимы для анализа защищенности ОИ?
3. Каким образом определяется факт защищенности?
4. Назвать и охарактеризовать типы и категории нарушителей.
5. Перечислить основные действия, которые может совершить внешний нарушитель.
6. Каким образом оценивается опасность каждой угрозы?
7. Что подразумевают под частотой (вероятностью) реализации угрозы? Назовите вербальные градации этого показателя.
8. Дать определение понятия «модель угроз безопасности». Назвать основные показатели, определяющие актуальность угроз.

4. Содержание отчёта

Отчёт обучающегося должен содержать:

— титульный лист,

— цель работы,

— выполнение заданий,

— краткий вывод,

— ответы на контрольные вопросы

5. Библиографический список

1. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов – 3-е изд., стер. – Москва: Академия, 2008. – 331 с.
2. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т.Р. Методы и средства инженерно-технической защиты информации: учебное пособие. 2-е изд., стер. - М.: Флинта, 2011. - 187 с.
3. Чипига А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие – М.: Гелиос АРВ, 2010. – 336 с.
4. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие – Брянск: БГТУ, 2005. – 269 с.
5. Аверченков, В.И. Организационная защита информации: учеб. пособие – Брянск: БГТУ, 2010. – 184 с.
6. ГОСТ Р 51624-00 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
7. ГОСТ Р 51275-99 Защита информации. Объект информатизации, факторы, воздействующие на информацию. Общие положения.
8. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 254 с.
9. Федеральный закон № 149-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
10. Федеральный закон № 152-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
11. Грибунин В.Г., Чудовский В.В. КСЗИ на предприятии. – М.: Академия, 2009. – 416 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Анализ типовых уязвимостей распределенных информационных систем

Методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03

Курск 2022

УДК 004.056.55

Составители: О.А. Демченко

Рецензент

Кандидат технических наук, доцент *А.Л. Марухленко*

Анализ типовых уязвимостей распределенных информационных систем: методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т; сост. О.А. Демченко Курск, 2022. - 12 с.

Содержат сведения по вопросам информационной безопасности. Указывается порядок выполнения лабораторной работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания разработаны для изучения дисциплин, связанными с безопасностью эксплуатации телекоммуникационных систем.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл.печ. л._____ . Уч.-изд.л _____. Тираж 30 экз. Заказ_____.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1. Краткие теоретические сведения

Под угрозой безопасности понимаются потенциально возможные воздействия, события, процессы или явления, которые прямо или косвенно могут нанести ущерб интересам субъектов информационных отношений.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в компьютерной системе (КС). С понятием угрозы безопасности тесно связано понятие уязвимости КС.

Уязвимость КС — это некоторое наиболее ранимое свойство системы, которое делает возможным возникновение и реализацию угрозы.

Атака на компьютерную систему — это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы. Таким образом, атака — это реализация угрозы безопасности.

Основная цель защиты КС — противодействие угрозам безопасности.

Источники угроз безопасности

Основными источниками угроз безопасности КС и информации (угроз интересам субъектов информационных отношений) являются:

• стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т. п.);

• сбои и отказы оборудования (технических средств) КС;

• последствия ошибок проектирования и разработки компонентов КС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);

• ошибки эксплуатации (пользователей, операторов и другого персонала);

• преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Естественные угрозы — это угрозы, вызванные воздействиями на КС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы — это угрозы КС, вызванные деятельностью человека. Среди искусственных угроз, исходя из мотивации действий, можно выделить:

• непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании КС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;

• преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к КС могут быть внешними или внутренними.

Классификация угроз безопасности

Выше мы рассмотрели два основных класса потенциальных угроз по природе их возникновения: естественные и искусственные. Но наряду с этим угрозы можно классифицировать и по различным аспектам реализации.

Классификация угроз по цели:

— несанкционированное чтение информации,

— несанкционированное изменение информации,

— несанкционированное уничтожение информации,

— полное или частичное разрушение КС (от кратковременного вывода из строя отдельных модулей до физического стирания системных файлов);

Классификация угроз по принципу воздействия на КС:

— использование легальных каналов получения информации (например, несанкционированное чтение из файла),

— использование скрытых каналов получения информации (например, недокументированных возможностей ОС),

— создание новых каналов получения информации (например, с помощью программных закладок).

Классификация угроз по характеру воздействия на КС:

— активное воздействие – несанкционированные действия в системе,

— пассивное воздействие – несанкционированное наблюдение за процессами в системе.

Классификация угроз по типу используемой слабости защиты:

— неадекватная политика безопасности (в том числе ошибки администратора),

— ошибки и недокументированные возможности ПО (так называемые «люки» - встроенные в систему специальные входы, предназначенные для тестирования или отладки, но случайно оставленные, что позволяет обходить систему защиты),

— ранее внедренные программные закладки.

Классификация угроз по способу воздействия на объект атаки:

— непосредственное превышение пользователем своих полномочий,

— работа от имени другого пользователя или перехват результатов его работы.

Классификация угроз по способу действий нарушителя (злоумышленника):

— в интерактивном режиме (вручную),

— в пакетном режиме (с помощью специальных программ, без участия пользователя).

Классификация угроз по используемым средствам атаки:

— штатные средства без использования дополнительного ПО,

— ПО третьих фирм (вирусы, вредоносные программы; ПО, разработанное для других целей – отладчики, сетевые мониторы и т. д.).

Классификация угроз по объекту атаки:

— аппаратные средства (оборудование),

— программное обеспечение,

— данные,

— персонал.

Возможные пути реализации угроз безопасности для перечисленных объектов атаки представлены в приведенной ниже таблице.

Пути реализации угроз безопасности			
Объекты воздействия	Нарушение конфиденциальности информации	Нарушение целостности информации	Нарушение работоспособности системы
Аппаратные средства	НСД - подключение; использование ресурсов; хищение носителей	НСД - подключение; использование ресурсов; модификация, изменение режимов	НСД - изменение режимов; вывод из строя: разрушение
ПО	НСД - копирование; хищение; перехват	НСД, внедрение "троянского коня", "вирусов", "червей"	НСД – искажение; удаление: подмена
Данные	НСД - копирование; хищение; перехват	НСД - искажение; модификация	НСД - искажение; удаление; подмена
Персонал	Разглашение; передача сведений о защите; халатность	"Маскарад": вербовка; подкуп персонала	Уход с рабочего места: физическое устранение

В соответствии с требованиями Руководящих документов при проведении работ по аттестации безопасности ИС, включающих в себя предварительное обследование и анализ защищенности объектов

информатизации, заказчиком работ должны быть предоставлены следующие исходные данные:

- полное и точное наименование ОИ и его назначение. Характер обрабатываемой информации (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень ее секретности, определенный в соответствии с тем или иным перечнем (государственным, отраслевым, ведомственным, предприятия);

- организационная структура ОИ;

- перечень помещений, состав комплекса технических средств, входящих в ОИ, в которых (на которых) обрабатывается указанная информация. Особенности и схема расположения ОИ с указанием границ контролируемой зоны;

- структура программного обеспечения, используемого на аттестуемом ОИ и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией;

- общая функциональная схема ОИ, включая схему источников питания и режимы обработки защищаемой информации;

- наличие и характер взаимодействия с другими ОИ;

- состав и структура системы ЗИ на аттестуемом ОИ;

- перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом ОИ и

имеющих соответствующий сертификат, предписание на эксплуатацию;

- сведения о разработчиках системы ЗИ, наличие у сторонних разработчиков лицензий на проведение подобных работ;

- наличие на ОИ службы безопасности;

- наличие и основные характеристики физической защиты объекта (помещений, где обрабатывается защищаемая информация и хранятся носители информации);

- наличие проектной и эксплуатационной документации на ОИ и другие исходные данные по объекту, влияющие на ИБ.

Для оценки текущего положения дел с обеспечением безопасности наиболее значимо предоставление перечисленных ниже сведений об ОИ:

- нормативно-распорядительная документация по проведению регламентных работ и обеспечению политики безопасности, должностные инструкции, процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам, топология корпоративной сети, структура информационных ресурсов с указанием степени критичности или конфиденциальности каждого из них, размещение информационных ресурсов в ИС, организационная структура пользователей и обслуживающих подразделений, размещение линий передачи данных, схемы и характеристики систем электропитания и заземления объектов, используемые системы сетевого управления и мониторинга;

- проектная документация – функциональные схемы, описание автоматизированных функций, описание основных технических решений;

- эксплуатационная документация – руководства пользователей и администраторов, использующих программные и технические средства ЗИ.

Анализ рисков начинается с формализации системы приоритетов организации в области ИБ. Для оценки ценности ресурсов необходимо выбирать подходящую систему критериев. Критерии должны позволять описать потенциальный ущерб, связанный с нарушением конфиденциальности, целостности, доступности.

Кроме критериев, учитывающих финансовые потери, в коммерческих организациях могут присутствовать критерии, отражающие:

- ущерб репутации организации;

- неприятности, связанные с нарушением действующего законодательства;

- ущерб для здоровья персонала;

- ущерб, связанный с разглашением персональных данных отдельных лиц;

- финансовые потери от разглашения информации;

- финансовые потери, связанные с восстановлением ресурсов;

- потери, связанные с невозможностью выполнения обязательств;

- ущерб от дезорганизации деятельности.

В правительственных учреждениях могут добавляться критерии, отражающие такие области, как национальная безопасность и международные отношения. Затем производится выбор подходящей технологии анализа рисков. Существуют различные подходы к оценке рисков.

Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму ИБ, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Минимальным требованиям к режиму ИБ соответствует базовый уровень ИБ. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, НСД и т. д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности их осуществления и уязвимости ресурсов.

Повышенные требования. В случаях, когда нарушения режима ИБ чреваты тяжелыми последствиями, базовый уровень требований к режиму ИБ является недостаточным. Для того чтобы сформулировать дополнительные требования, необходимо:

- определить ценность ресурсов;

- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

- оценить вероятность угроз;

- определить уязвимость ресурсов.

Исходными данными являются результаты опроса сотрудников, базы данных со статистикой по классам рисков. В результате выполнения этого этапа должен быть написан документ "Анализ рисков".

Для базового уровня ИБ документ будет содержать раздел: "Классы рисков, принимаемых во внимание при построении подсистемы ИБ".

Для повышенного уровня ИБ документ будет содержать разделы:

- «Оценка ценности информационных ресурсов»;

- «Возможные пути нарушения режима ИБ (модель угроз)»;

- «Модель нарушителя по выбранным классам угроз»;

- «Оценка параметров угроз и уязвимых мест ИС».

Выделяется четыре подхода к управлению рисками:

1. Уменьшение риска. Многие риски могут быть существенно уменьшены путем использования весьма простых и дешевых контрмер. Например, грамотное управление паролями снижает риск НСД.

2. Уклонение от риска. От некоторых классов рисков можно уклониться. Например, вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска НСД в локальную сеть со стороны Web-клиентов.

3. Изменение характера риска. Если не удается уклониться от риска или эффективно его уменьшить, можно принять некоторые меры страховки.

4. Принятие риска. Многие риски не могут быть уменьшены до пренебрежимо малой величины. На практике, после принятия стандартного набора контрмер, ряд рисков уменьшается, но остается все еще значимым. Необходимо знать остаточную величину риска.

Исходными данными являются результаты опроса сотрудников, экспертные оценки возможности применения стандартных подходов к управлению рисками. В результате выполнения этапа для принимаемых во

внимание рисков должна быть предложена стратегия управления, излагаемая в документе "Управление рисками":

- выделение рисков, уровень которых недопустимо высок;
- стратегия управления рисками;
- выбор варианта контрмер.

2. Индивидуальное задание студента

В данной работе изучается анализ рисков информационной безопасности.

Цель работы: ознакомиться с алгоритмами и произвести оценку рисков информационной безопасности.

Этапы работ

1. Загрузить ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.

2. Ознакомьтесь с Приложениями C, D и E ГОСТа Р ИСО/МЭК ТО 13335-3-2007.

3. В соответствии с вариантом выберите три различных информационных актива организации.

4. Из Приложения D ГОСТа Р ИСО/МЭК ТО 13335-3-2007 подберите три конкретных уязвимости системы защиты указанных информационных активов.

5.Пользуясь приложением C ГОСТа Р ИСО/МЭК ТО 13335-3-2007 напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов (см. вариант) предложенных в Приложении E ГОСТа Р ИСО/МЭК ТО 13335-3-2007 произведите оценку рисков информационной безопасности. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Вариант в соответствии с номером по журналу.

Номер варианта	Организация	Метод оценки риска (см. Приложение Е ГОСТа)
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2

3. Контрольные вопросы

1. Что включает в себя типовая методика анализа защищенности ИС предприятия?
2. Какие исходные данные необходимы для анализа защищенности ОИ?
3. Назовите основные критерии оценки рисков.
4. Какие существуют подходы к оценке рисков?
5. Какие типовые разделы должен содержать документ "Анализ рисков"?
6. Какие существуют подходы к управлению рисками?
7. Как определить риски через коэффициенты значимости?
8. Каким образом определяется факт защищенности?

4. Содержание отчёта

Отчёт обучающегося должен содержать:

— титульный лист,

— цель работы,

— выполнение заданий,

— краткий вывод,

— ответы на контрольные вопросы

5. Библиографический список

1. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов – 3-е изд., стер. – Москва: Академия, 2008. – 331 с.
2. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т.Р. Методы и средства инженерно-технической защиты информации: учебное пособие. 2-е изд., стер. - М.: Флинта, 2011. - 187 с.
3. Чипига А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие – М.: Гелиос АРВ, 2010. – 336 с.
4. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие – Брянск: БГТУ, 2005. – 269 с.
5. Аверченков, В.И. Организационная защита информации: учеб. пособие – Брянск: БГТУ, 2010. – 184 с.
6. ГОСТ Р 51624-00 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
7. ГОСТ Р 51275-99 Защита информации. Объект информатизации, факторы, воздействующие на информацию. Общие положения.
8. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 254 с.
9. Федеральный закон № 149-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
10. Федеральный закон № 152-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
11. Грибунин В.Г., Чудовский В.В. КСЗИ на предприятии. – М.: Академия, 2009. – 416 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Сетевые и узловые системы анализа защищенности

Методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03

Курск 2022

УДК 004.056.55

Составители: О.А. Демченко

Рецензент

Кандидат технических наук, доцент *А.Л. Марухленко*

Сетевые и узловые системы анализа защищенности: методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т; сост. О.А. Демченко
Курск, 2022. - 12 с.

Содержат сведения по вопросам информационной безопасности. Указывается порядок выполнения лабораторной работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания разработаны для изучения дисциплин, связанными с безопасностью эксплуатации телекоммуникационных систем.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл.печ. л._____ . Уч.-изд.л _____. Тираж 30 экз. Заказ_____.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1. Краткие теоретические сведения

Сканер безопасности XSpider является разработкой фирмы Positive Technologies.

В отличии от сканера NMap, сканер XSpiderимеет удобный графический интерфейс, более интеллектуальные алгоритмы поиска уязвимостей, большую обновляемую базу уязвимостей, а также возможность создания полноценных отчетов по безопасности системы и многое другое.

Есть ряд особенностей, которые дают преимущества сканеру XSpider как системе анализа защищенности над другими продуктами данного класса. Как подчеркивают сами разработчики, главная особенность XSpider — это его сканирующее ядро, которое способно имитировать сценарий поведения потенциального злоумышленника. Также следует отметить мощную "интеллектуальную начинку" XSpider, которая реализуется во встроенных эвристических алгоритмах, позволяющих надежно идентифицировать еще не опубликованные новые уязвимости.

Особенности сканирующего ядра

— Полная идентификация сервисов на случайных портах

— Дает возможность проверки на уязвимость серверов со сложной нестандартной конфигурацией, когда сервисы имеют произвольно выбранные порты

— Эвристический метод определения типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH) вне зависимости от их ответа на стандартные запросы

— Служит для определения настоящего имени сервера и корректной работы проверок в тех случаях, если конфигурация WWW-сервера скрывает его настоящее имя или заменяет его на другое

— Обработка RPC-сервисов (Windows и *nix) с их полной идентификацией

— Обеспечивает возможности определения RPC-сервисов и поиска уязвимостей в них, а также определения детальной конфигурации компьютера в целом

— Проверка слабости парольной защиты

— Производится оптимизированный подбор паролей практически во всех сервисах, требующих аутентификации, помогая выявить слабые пароли

— Глубокий анализ контента WEB-сайтов

— Анализ всех скриптов HTTP-серверов (в первую очередь, пользовательских) и поиск в них разнообразных уязвимостей: SQL инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP Response Splitting.

— Анализатор структуры HTTP-серверов

— Позволяет осуществлять поиск и анализ директорий доступных для просмотра и записи, давая возможность находить слабые места в конфигурации

— Проведение проверок на нестандартные DoS-атаки

— Существует возможность включения проверок "на отказ в обслуживании", основанных на опыте предыдущих атак и хакерских методах

— Специальные механизмы, уменьшающие вероятность ложных срабатываний

— В различных видах проверок используются специально под них разработанные методы, уменьшающие вероятность ошибочного определения уязвимостей

— Ежедневное добавление новых уязвимостей и проверок

— Оригинальная технология обновления программы не только позволяет пользователям каждый день иметь актуальную базу уязвимостей при минимальном трафике и временных затратах не прекращая при этом

работы программы, но и обеспечивает регулярный update программных модулей по мере их совершенствования.

Надежность

— Надежность работы при нестандартных конфигурациях ПО

— Надежность работы при низком качестве TCP-связи

— Возможность определять еще не опубликованные уязвимости при помощи интеллектуальных эвристических алгоритмов.

— Крайне низкая вероятность пропуска существующей уязвимости

Интерфейс XSpider 7.8

Окно управления сканированиями показано на рисунке 1.

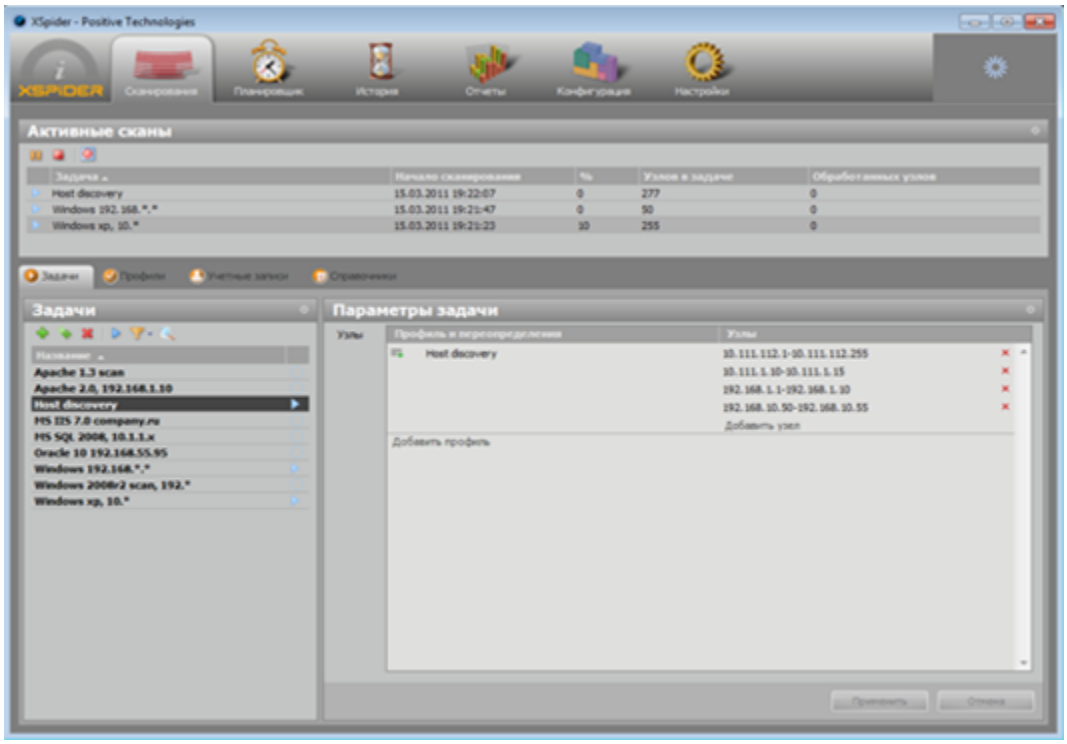

Рис.1 — Окно управления сканированиями

Окно документа сканирования показано на рисунке 2.

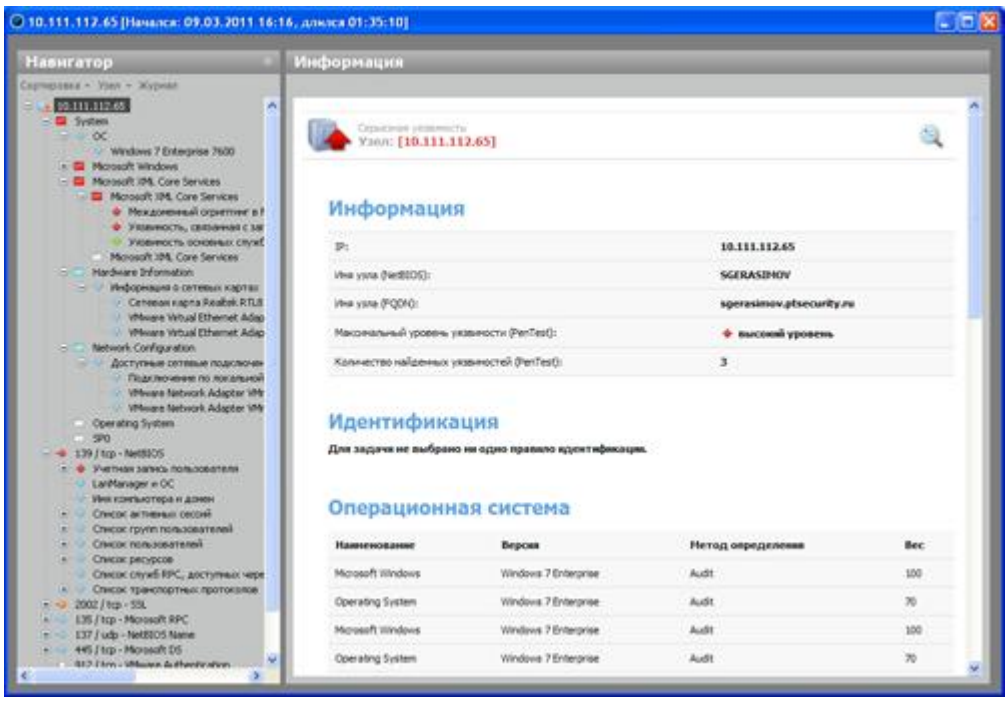

Рис.2 — Окно документа сканирования

Диалог создания отчета представлен на рисунке 3.

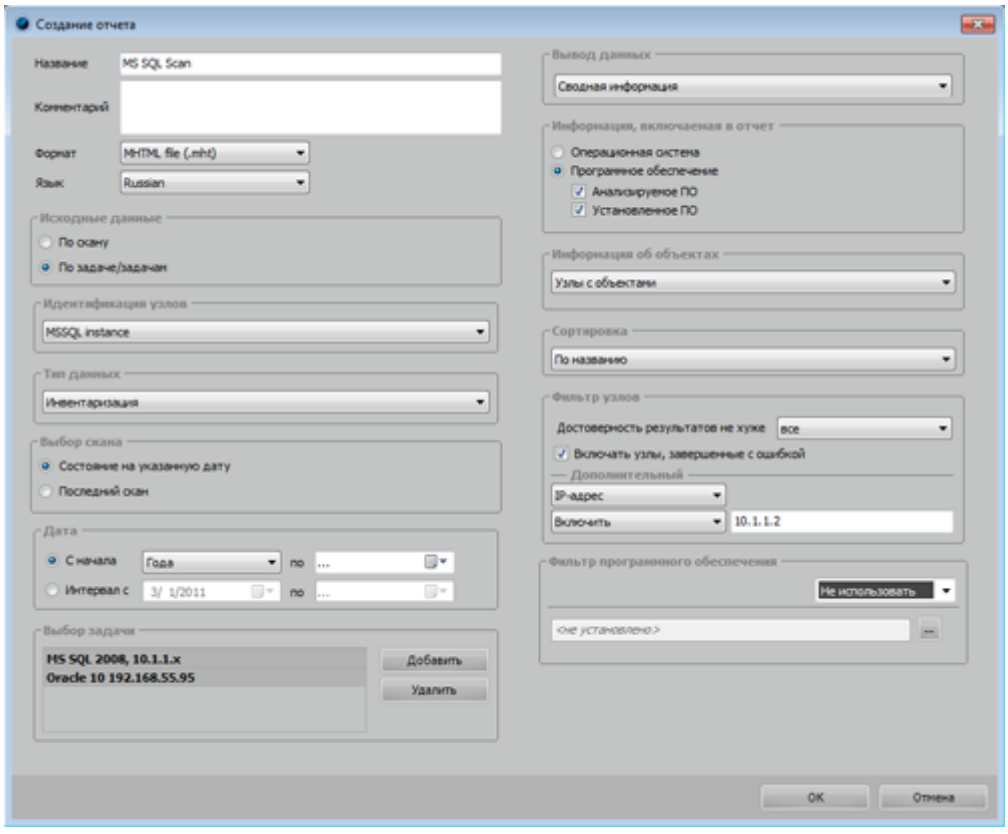

Рис.3 — Диалог создания отчета

2. Индивидуальное задание студента

Задание 1

Найти и описать 3-5 уязвимостей разного типа при помощи сканера X-Spider, определить их опасность и потенциальную угрозу, пояснить пути устранения.

Ход работы.

1. Необходимо скачивать версию программы X-spider и установить её. Хотя XSpider работает под управлением Microsoft Windows, но он проверяет все возможные уязвимости независимо от программной и аппаратной платформы узлов: начиная от рабочих станций под Windows и кончая сетевыми устройствами Cisco.

2. Запустить программу XSpider. «Сканируемые хосты» и вводим имя или IP-адрес компьютера, который надо сканировать на наличие уязвимостей. Процесс сканирования занимает 5-15 минут в среднем.

3. После сканирования компьютера XSpider указывает уязвимости, выявляем серьёзные уязвимости (отмеченные красными точками). Отметьте уязвимости, которые вы нашли. Если такие уязвимости уже отмечены другими, то необходимо повторить сканирование, но уже для другого случайно выбранного компьютера.

4. Описать найденную уязвимость, её угрозу для информационной безопасности. А также необходимо описать решение, которое необходимо для устранения данной уязвимости.

Задание 2

Совместный режим. Каждый студент должен работать в паре с другим студентом.

1.Запустить утилиту сканирования сети XSpider;

2.В меню «Правка» выбрать «Добавить хост»;

3.Введите IP-адрес хоста напарника;

4.Узнать у напарника текущий режим работы МСЭ;

5.В меню «Сканирование» выберите «Старт все»;

Начнется попытка XSpider сканировать указанный хост. В случае, если на целевом хосте отключены ICMP-ответы, то сканирование происходить не будет без установки в XSpider специальной опции: меню «Профиль» -> «Редактировать текущий» -> «Поиск хостов» -> поставить галочку «Сканировать не отвечающие хосты».

6. Сбросить флаг «Сканировать не отвечающие хосты» для возврата XSpider в первоначальную конфигурацию.

3. Контрольные вопросы

1. Для чего нужен сканер безопасности?
2. Какую роль могут сыграть открытые порты в создании угроз информационной безопасности?
3. Назовите основные способы устранения сетевых уязвимостей?
4. Какие виды сканеров уязвимости можно выделить?
5. При помощи каких двух два основных механизмов сканер проверяет наличие уязвимости?
6. Опишите этапы сканирования.

4. Содержание отчёта

Отчёт обучающегося должен содержать:

— титульный лист,

— цель работы,

— выполнение заданий,

— краткий вывод,

— ответы на контрольные вопросы

5. Библиографический список

1. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов – 3-е изд., стер. – Москва: Академия, 2008. – 331 с.
2. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т.Р. Методы и средства инженерно-технической защиты информации: учебное пособие. 2-е изд., стер. - М.: Флинта, 2011. - 187 с.
3. Чипига А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие – М.: Гелиос АРВ, 2010. – 336 с.
4. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие – Брянск: БГТУ, 2005. – 269 с.
5. Аверченков, В.И. Организационная защита информации: учеб. пособие – Брянск: БГТУ, 2010. – 184 с.
6. ГОСТ Р 51624-00 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
7. ГОСТ Р 51275-99 Защита информации. Объект информатизации, факторы, воздействующие на информацию. Общие положения.
8. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 254 с.
9. Федеральный закон № 149-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
10. Федеральный закон № 152-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
11. Грибунин В.Г., Чудовский В.В. КСЗИ на предприятии. – М.: Академия, 2009. – 416 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Сетевые и узловые системы обнаружения и предотвращений вторжений

Методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03

Курск 2022

УДК 004.056.55

Составители: О.А. Демченко

Рецензент

Кандидат технических наук, доцент *А.Л. Марухленко*

Сетевые и узловые системы обнаружения и предотвращений вторжений: методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т; сост. О.А. Демченко Курск, 2022. - 9 с.

Содержат сведения по вопросам информационной безопасности. Указывается порядок выполнения лабораторной работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания разработаны для изучения дисциплин, связанными с безопасностью эксплуатации телекоммуникационных систем.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл.печ. л._____ . Уч.-изд.л _____. Тираж 30 экз. Заказ_____.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1. Краткие теоретические сведения

Цель работы: изучение эффективности использования систем обнаружения вторжений для защиты от сетевых атак.

Система обнаружения вторжений - это программное или программно-аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть, обнаружения фактов сканирования портов, атак на отказ в обслуживании или переполнения буфера (различных способов удаленного вредоносного воздействия на защищаемый компьютер, когда на самом объекте атаки никакого кода не остается, но требуемое нарушителю действие выполняется) и детектирования атак других типов. Основное различие в методах работы систем обнаружения вторжений и сетевых экранов заключаются в следующем.

Сетевой экран задерживает или пропускает пакеты в соответствии с имеющимися у него правилами фильтрации. Сетевой экран может пропустить атаку, если она выполняется по правилам, разрешающим (с точки зрения самого сетевого экрана) взаимодействие между компьютерами.

В отличие от сетевого экрана, система обнаружения вторжений осуществляет свою деятельность, используя эвристические алгоритмы.

При этом происходит обработка пакетов, получаемых от всех компьютеров. По этой причине следует, наряду с системами обнаружения вторжений, использовать сетевые экраны. Они будут блокировать попытки соединения с компьютерами, взаимодействие с которыми заведомо не предусмотрено для защищаемого объекта, то есть осуществлять «грубую фильтрацию».

Таким образом, будет снижена нагрузка на систему обнаружения вторжений, главной задачей которой является обнаружение возможных сетевых вторжений. Обычно система обнаружения вторжений состоит из следующих частей:

- подсистемы индикаторов или сенсоров. Они используются для сбора событий, связанных с обеспечением безопасности защищаемой системы;

- аналитической подсистемы, выявляющей атаки и подозрительные действия. Работа аналитической подсистемы основана на сведениях, зафиксированных индикаторами;

- базы данных, где хранятся сведения о накопленных с использованием индикаторов событий и результатов их анализа;

- консоли, позволяющей настраивать систему обнаружения вторжений, наблюдать за ее состоянием, просматривать события.

Как правило, сетевая атака начинается со сканирования портов, что позволяет получить максимально возможную информацию об объекте нападения. Затем нарушитель, используя полученную в ходе сканирования информацию, определяет уязвимости объекта и выбирает методы их атаки. Третий этап представляет собой собственно атаку - попытку применения выбранных эксплойтов для нанесения ущерба информационной и программной среде жертвы. Поэтому задачей системы обнаружения вторжений является противодействие как сканированию, так и применению эксплойтов.

2. Задание лабораторной работы

Выполнить:

- анализ двух сетевых или узловых систем обнаружения и предотвращений вторжений. Сделать таблицу.
- углубить и уточнить представления о сетевых уязвимостях, их выявлении, исправлении и роли в обеспечении информационной безопасности.
-

3. Контрольные вопросы

1. Что такое уязвимость и угроза сетевого узла?
2. В связи с чем возникают уязвимости?
3. Что такое сканер безопасности и для чего он служит?
4. Законно ли применение сканера безопасности?
5. В чем принцип работы сканера безопасности?
6. Какие сложности могут возникнуть при оценке безопасности?
7. Перечислите классы сканеров безопасности и охарактеризуйте их.
8. Перечислите недостатки сканеров безопасности.
9. Являются ли сканеры безопасности абсолютно надежным способом анализа безопасности сетевой компьютерной системы?
10. Каковы основные возможности программы NMap?
11. К какому классу сканеров возможно отнести программу NMap?
12. Перечислите основные методы сканирования программы NMap. Какие дополнительные возможности присутствуют в NMap?
13. Каковы результаты работы программы NMap?
14. Каковы отличительные особенности сканера XSpider от других?

4. Содержание отчёта

Отчёт обучающегося должен содержать:

— титульный лист,

— цель работы,

— выполнение заданий,

— краткий вывод,

— ответы на контрольные вопросы

5. Библиографический список

1. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов – 3-е изд., стер. – Москва: Академия, 2008. – 331 с.
2. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т.Р. Методы и средства инженерно-технической защиты информации: учебное пособие. 2-е изд., стер. - М.: Флинта, 2011. - 187 с.
3. Чипига А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие – М.: Гелиос АРВ, 2010. – 336 с.
4. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие – Брянск: БГТУ, 2005. – 269 с.
5. Аверченков, В.И. Организационная защита информации: учеб. пособие – Брянск: БГТУ, 2010. – 184 с.
6. ГОСТ Р 51624-00 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
7. ГОСТ Р 51275-99 Защита информации. Объект информатизации, факторы, воздействующие на информацию. Общие положения.
8. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 254 с.
9. Федеральный закон № 149-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
10. Федеральный закон № 152-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.
11. Грибунин В.Г., Чудовский В.В. КСЗИ на предприятии. – М.: Академия, 2009. – 416 с.