Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Н. Я. Великите

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Учебно-методическое пособие по изучению дисциплины
для студентов магистратуры по направлению подготовки
15.04.04 Автоматизация технологических процессов и производств

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.056.57(076)

Рецензент
кандидат технических наук, доцент кафедры теории машин и механизмов и деталей машин ФГБОУ ВО «Калининградский государственный технический университет» О. С. Витренко

Великите, Н. Я.
Информационная безопасность автоматизированных систем: учебно-методическое пособие по изучению дисциплины для студентов магистратур по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 49 с.

Учебно-методическое пособие является руководством к изучению дисциплины «Информационная безопасность автоматизированных систем». В документе представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, указания к изучению каждой темы. Вопросы для изучения методических материалов к занятию, методические указания по выполнению самостоятельной работы. Содержатся требования к текущей и промежуточной аттестации.
Табл. 2, рис. 7, список лит. – 14 наименований

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий 29 апреля 2025 г., протокол № 3

УДК 004.056.57(076)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Целью изучения дисциплины является: формирование знаний, умений и навыков, необходимых для знания и определения основных уязвимостей открытых информационных систем.

Задачей преподавания дисциплины, отражающейся в ее содержании, является формирование целостного представления обучающегося о широкой сфере проблем обеспечения информационной безопасности в автоматизированных системах в рамках изучения двух разделов согласно тематического плана дисциплины «Информационная безопасность автоматизированных систем». Раздел 1. Общие вопросы информационной безопасности. Раздел 2. Современное состояние обеспечения информационной безопасности в автоматизированных системах.

При изучении данной дисциплины студент будет:

знать:

– концепцию диспетчера доступа;

– методы и средства ограничения доступа к ресурсам;

– методы и средства обнаружения уязвимостей;

– методы и средства обнаружения атак на ресурсы;

– методы и средства противодействия атакам на ресурсы;

уметь:

– организовывать защиту; производить защиту от атак на ресурсы;

– производить защиту программ от изменений; осуществлять контроль трафика;

владеть:

– средствами защиты от несанкционированного доступа и нарушения функциональности ее подсистем;

– средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных; методикой контроля информационной целостности.

Место дисциплины в структуре основной профессиональной образовательной программы: дисциплина «Информационная безопасность автоматизированных систем» является дисциплиной части, формируемой участниками образовательных отношений Модуля по выбору 1. Информационное моделирование. «Модуль по выбору 1. Информационное моделирование» относится к блоку 1 и включает в себя четыре дисциплины, одной из которых является дисциплина «Информационная безопасность автоматизированных систем»

Общая трудоемкость дисциплины составляет 4 зачетных единиц (з.е.), т. е. 144 академических часов контактной и самостоятельной учебной работы студента; работы, связанной с текущей и промежуточной аттестацией по дисциплине.

Основными видами аудиторных учебных занятий по дисциплине являются лекции и лабораторные занятия.

Формирование знаний, обучающихся обеспечивается проведением лекционных занятий.

В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешением их, как непосредственно в ходе занятий, так и в ходе самостоятельной работы.

Контроль знаний в ходе изучения дисциплины осуществляется в виде текущего контроля, а также промежуточной аттестации в форме зачета.

Текущий контроль (контроль выполнения заданий на самостоятельную работу) предназначен для проверки хода и качества усвоения студентами учебного материала и стимулирования их учебной работы. Он может осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины.

Текущий контроль предполагает постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Их результаты учитываются выставлением преподавателем оценок в журнале учета успеваемости и в ходе ежемесячной аттестации.

При текущем контроле успеваемости учитывается: выполнение обучающимся всех работ и заданий, предусмотренных рабочей программой дисциплины, а именно выполнение заданий на лабораторных занятиях; самостоятельную работу обучающихся; посещаемость аудиторных занятий.

Далее в пособии представлены методические материалы по изучению дисциплины, включающие тематический план занятий с перечнем вопросов для изучения, рекомендуемой литературой, методическими указаниями.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделе ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

В учебно-методическом материале по изучению дисциплины представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины.

В разделе содержание дисциплины приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропус-

ка каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Контроль и аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету.

Перечень программного обеспечения:

– ОС AstraLinux;

– OpenOffice;

– Mozilla, Wireshark, Suricata, программное обеспечение «Киберполигон» (Security Onion, IDSNSVipNet, TIAS, и др. в рамках лицензии на «Киберполигон»).

2. ТЕМАТИЧЕСКИЙ ПЛАН

Тематический план изучения дисциплины «Информационная безопасность автоматизированных систем» представлен в таблице 1.

Таблица 1 –Тематический план изучения дисциплины «Информационная безопасность автоматизированных систем»

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лекции		
1	Общие вопросы информационной безопасности	Тема 1. Введение. Термины и определения	4	5
		Тема 2. Стандарты информационной безопасности	4	5
2	Современное состояние обеспечения информационной безопасности в автоматизированных системах	Тема 3. Основные регуляторы в области ИБ. Обзор некоторых Интернет-ресурсов в помощь к изучению вопросов информационной безопасности	4	5
		Тема 4. Технологии информационной безопасности автоматизированных систем и техническая защита информации	4	5
		Тема 5. Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire» (Киберполигон)	4	5
		Тема 6. Введение в изучение среды моделирования «Киберполигон» для исследования атак с использованием средств обнаружения вторжений	10	10
			30	**35**
		Лабораторные занятия		
1	Общие вопросы информационной безопасности	Занятие 1. Парольная защита. Количественные оценки парольной защиты	5	7
		Взлом пароля архива программой AP, Hydra	5	7

2	Современное состояние обеспечения информационной безопасности в автоматизированных системах	Занятие 2. Применение технологий информационной безопасности автоматизированных систем с использованием виртуального программного обеспечения компании DokiSun. Часть 1 Виртуальное ПО Криптография. Часть 2 Виртуальное ПО системы контроля управления данными (СКУД)	10	7
		Занятие 3. Рассмотрение технологий защиты информации по индивидуальному заданию преподавателя на примере использования среды моделирования «Киберполигон»	10	14
			30	**35**
		Рубежный (текущий) и итоговый контроль		
1	Общие вопросы информационной безопасности	Тестирование (ЭИОС)	6 (РЭ)	7
		Зачёт	0,15 (КА)	0,85
			66,15	**77,85**
		Всего		**144**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Раздел 1. Общие вопросы информационной безопасности

3.1.1 Тема 1 Введение. Термины и определения

Перечень изучаемых вопросов

1.История развития теории и практики обеспечения информационной безопасности

2.Содержание и структура понятия информационной безопасности

3.Общая характеристика принципов, методов и механизмов обеспечения информационной безопасности

Методические указания к изучению

В данной теме мы рассмотрим предмет и задачи дисциплины. Дадим определение ИБ из Доктрины Информационной безопасности РФ, утвержденной Указом Президента Российской Федерации 6 декабря 2016 г. Сделаем исторический экскурс по этапам развития методов и средств обеспечения безопасности информации. В вопросе содержание и структура понятия ИБ рассмотрим три основных свойства информации: конфиденциальность, целостность, доступность.

Особое внимание следует обратить на определения угроз и их классификацию. Дадим определение автоматизированной системы, несанкционированный доступ, угроза, источники угроз, уязвимость информации, политика безопасности, познакомимся с перечнем сокращений широко применяемых в ИБ: НСД, АС, БД, СЗИ, ПЭМИН, ЦЗИ и рассмотрим др. понятия, которые более подробно изложены в лекционном материале в виде презентаций в среде ЭИОС.

Приведём только некоторые термины из алфавитного списка понятий по информационной безопасности:

АВТОРИЗАЦИЯ – предоставление определенных полномочий лицу (группе лиц) на выполнение некоторых действий в системе обработки данных.

АДМИНИСТРАТОР базы данных (БД) – Специальное должностное лицо (группа лиц), имеющее полное представление о БД и отвечающее за ее ведение, использование и развитие А. защиты – субъект доступа, ответственный за защиту автоматизированной системы от НСД к информации

АККРЕДИТАЦИЯ – авторизация и санкционирование возможности об работки критичных данных в операционной среде информационной системы или сети. Решение об А. выносится после получения всеми лицами из технического персонала сертификата, подтверждающего возможность этих лиц работать с защищенными системами

АКТУАЛИЗАЦИЯ – процесс, обеспечивающий постоянное внесение текущих изменений в состояние системы, базы данных

АНАЛИЗ трафика – (рабочей нагрузки) линии связи – исследование наблюдаемых потоков данных, проходящих между пунктами по сети связи (наличие, отсутствие, объем, направление, частота)

АНТИВИРУСНЫЕ программы – программы, предотвращающие заражение компьютерным вирусом и ликвидирующие последствия заражения

АТТЕСТАЦИЯ средств защиты – удостоверение степени соответствия требованиям к данному классу средств защиты

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекта доступа предъявленного им идентификатора, подтверждение подлинности А. пользователя – проверка соответствия пользователя предъявляемому им идентификатору.

БАГ (англ. bug – жук) – жаргонное слово, обозначающее ошибку в программе. Термин обычно употребляется в отношении ошибок, проявляющих себя на стадии работы программы, в отличие, например, от ошибок проектирования или синтаксических ошибок.

БАГТРАК (англ. Bugtraq) – лента новостей (сайты или списки рассылки) об уязвимостях в программном обеспечении. Обновляется каждый месяц.

БАРЬЕР информационный – совокупность различных препятствий, возникающих на пути распространения и использования информации

Б. психологический – возникает между пользователем и новой системой, вызывается, как правило, боязнью трудностей при переходе на новую систему, неизвестностью того, будет ли она понятна и лучше старой

БЕЗВРЕДНЫЕ вирусы – это вирусы, никак не влияющие на работу компьютера. Они не разрушают файлы, но могут переполнять оперативную и дисковую память, выводить на экран графические эффекты и т. д.

БЕЗОПАСНОСТЬ Б. данных – свойство КС противостоять попыткам НСД к обрабатываемой и хранимой информации. Б. достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий. Одним из показателей Б. является безопасное время.

Б. информации – состояние защищенности информации, обрабатываемой средствами ВТ, или автоматизированной системы от внутренних или внешних угроз.

Б. компьютерных систем – свойство КС противостоять попыткам НСД к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, и навязыванию ложной информации Б. субъектов информационных отношений – защищенность субъектов информационных от-

ношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

БРАНДМАУЭР – сочетание программного и аппаратного обеспечения, образующее систему защиты от несанкционированного доступа к компьютеру из внешней глобальной или локальной сети

ВЕРИФИКАЦИЯ – 1/ процесс сравнения двух уровней спецификации средств ВТ или АС на надлежащее соответствие; 2/ в программировании – доказательство правильности программ. Различают два подхода к верификации: статический и конструктивный.

ВИРУС – программа, способная самопроизвольно создавать свои копии и модифицирующая другие программы, записанные в файлах или системных областях, для последующего получения управления и воспроизводства новой копии. Часто содержит бомбы или создает различные аудио- и видео эффекты. Переносится при копировании программ. Либо через дискеты, с которыми работали на зараженном компьютере.

ВИРУСЫ-репликаторы (черви). Распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии (от англ. Replicators – объекты, которые копируют сами себя)

ВЛАДЕЛЕЦ – в системе ЗИ и контроля доступа – пользователь, имеющий неограниченные права по отношению к файлу или другой информации.

ВРЕМЯ Безопасное В. – математическое ожидание времени раскрытия системы защиты статистическим опробированием возможных вариантов доступа к данным. Вычисляется по формуле: n T = ∑ i = 1 p i t i , где n – число проб, pi – вероятность раскрытия при i-й пробе, ti – время, затрачиваемое на i-ю пробу.

Среднее В. безотказной работы – среднестатистическая продолжительность нормального функционирования технического устройства между двумя последовательными отказами.

ВЫЗОВ – санкционированный В. – вызов системы, программы или данных. раз решенный данному пользователю. Как правило, реализуется путем ввода и проверки пароля.

ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ – это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

ФЛАГ – часть формата элемента данных из одного или нескольких битов, которые определяют его статус.

ФРИКИНГ (англ. phreaking) – сленговое выражение, означающее взлом телефонных автоматов и сетей, обычно с целью получения бесплатных звонков.

ФРИКЕРЫ (англ. phreaker). – люди, специализирующихся на фрикинге. Это же название применяют к людям, использующим в своих неправомерных действиях телефон с целью оказать психологическое воздействие на конечного абонента.

ХАКЕР – пользователь, который пытается вносить изменения в системное ПО, не имея на это право. Этом может быть программист, который создает более или менее полезные вспомогательные программы, обычно плохо документированные и иногда вызывающие нежелательные побочные результаты

ЦЕЛОСТНОСТЬ – состояние данных или КС, в которой данные или программы используются установленным образом, обеспечивающим устойчивую работу системы, автоматическое восстановление в случае обнаружения системой потенциальной ошибки, автоматическое использование альтернативных компонентов вместо вышедших из строя.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – свойство информации, заключающееся в ее существовании в неизменном виде (по отношению к некоторому фиксированному ее состоянию) в условиях случайного и (или) преднамеренно го искажения (разрушения).

ЦЕННОСТЬ информации – свойство информации, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной деятельности человека.

ШИФР – криптографический прием, связанный с применением некоторого алгоритма преобразования символов (букв и цифр) исходного (незашифрованного) текста в зашифрованный код. Ш. ассиметричный – шифр, в котором ключ шифрования не совпадает с ключом дешифрования.

ШИФРОВАНИЕ – криптографическое преобразование данных для по лучения шифрованного текста.

ЭКСПЛОЙТ – это любая программа, разработанная с целью выявления или использования уязвимостей в другом ПО.

ЭЛЕКТРОННАЯ ПОДПИСЬ – компьютерный эквивалент обычной подписи под документом, который должен обеспечить подлинность документа и защитить передаваемое сообщение от изменений

ЭЛЕКТРОННЫЙ КЛЮЧ – устройство для защиты программных продуктов от незаконного тиражирования и использования

ЭХОКОНТРОЛЬ – метод контроля передачи данных, при котором принятые данные, возвращаются на передающий пункт и сравниваются с переданными данными.

ЯДРО защиты – технические программы и многопрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа

Рекомендуемая литература:[1, с. 5–26, 40–51]; [2, с. 9–25].

Контрольные вопросы для самопроверки

1. Что является предметом изучения дисциплины?
2. Были ли в вашей практике случаи попыток НСД к информации, обрабатываемой в АС?
3. Поясните отличие понятие компьютерной безопасности и информационной безопасности. Какое из понятий является более общим?
4. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?
5. Чем определяется стойкость подсистемы идентификации и аутентификации?
6. Перечислите минимальные требования к выбору пароля. Какой пароль является «плохим», а какой «хорошим»?
7. Назовите основные способы аутентификации. Какой из этих способов является, по вашему мнению, наиболее эффективным?
8. Дайте определение идентификации и аутентификации пользователей. В чём разница между этими понятиями?
9. Что такое авторизация?
10. Каковы основные принципы защиты от НСД? В чём суть каждого из этих принципов?

3.1.2 Тема 2 Стандарты информационной безопасности

Перечень изучаемых вопросов

1. Роль стандартов ИБ.
2. Международные и отечественные стандарты в области защиты персональных данных.

Методические указания к изучению

Стандарты информационной безопасности представляют собой набор правил и рекомендаций, направленных на обеспечение защиты информации от различных угроз

Современные, ускоренные темпы развития информационных технологий и нарастающее противостояние в обществе актуализируют проблемы информационной безопасности, и требует постоянного усовершенствования, не только

технической составляющей, но также создания эффективного правового и организационного сопровождения соответствующих процессов.

При изучении данной темы следует пользоваться системами «Консультант» и «Гарант», чтобы иметь возможность пользоваться актуальным материалами в рамках законодательства и нормативно-правовой базы.

Главной задачей стандартов ИБ является создание основы для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. *Особое внимание в рамках этой темы уделим стандартам информационной безопасности в области персональных данных*. Рассмотрены особенности стандартизации процесса обеспечения безопасности коммерческой информации в сетях с протоколами передачи данных IP/TCP, SMTP, POP, SNMP, SSL, SET, IPSec, PKI.

Среди различных стандартов по безопасности ИТ следует выделить нормативные документы по критериям оценки защищённости средств вычислительной техники и АС и документы регулирующие информационную безопасность.

При изучении данной темы мы познакомимся с понятиями: Коммерческая тайна, Государственная тайна, Обладатель информации, Гриф секретности, Степень секретности и др.

Согласно действующему законодательству (ч. 1, ст. 16 ФЗ РФ «Об информации, информационных технологиях и о защите информации») **защита информации** представляет собой принятие правовых, организационных и технических мер, направленных на предотвращение правонарушений в сфере информации

Персональными данными является любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (ч. 1, абз. 1, ст. 3 ФЗ «О персональных данных»).

К персональным данным могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам, а именно:

– биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода);

– личные особенности (в том числе о личных привычках и наклонностях);

– сведения о семейном положении (в том числе о семейных отношениях);

– сведения об имущественном, финансовом положении (кроме случаев, прямо установленных законом);

– сведения о состоянии здоровья.

Источники права в области персональных данных:

– Конституция РФ;

– ФЗ РФ «О персональных данных»;

– ФЗ РФ «Об информации, информационных технологиях и о защите информации»;

– международные НПА (Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR – General Data Protection Regulation с изменениями от 25.05.2018);

Согласно Федеральному закону «О персональных данных» государственными регуляторами являются:

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомназор) – уполномоченный орган по защите прав субъектов персональных данных, осуществляет контроль и надзор за соответствием обработки ПДн требованиям законодательства.

Согласно Федеральному закону «О персональных данных» государственными регуляторами по технической защите ПДн являются:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) – федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, устанавливает методы и способы защиты в информационных системах не криптографическими методами, осуществляет контроль выполнения установленных требований.

Федеральная служба безопасности (ФСБ России) – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, устанавливает методы и способы защиты в информационных системах криптографическими методами, осуществляет контроль выполнения установленных требований.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Правовой институт государственной тайны представляет собой совокупность правовых норм, регулирующих общественные отношения в сфере оборота информации ограниченного доступа, которая имеет особое значение для стабильности и безопасности государства.

В Европейском Союзе в отношении защиты персональных данных действуют нормы GDPR (General Data Protection Regulation, Общий регламент по защите персональных данных). Данный документ, принят в апреле 2016 г., вступил в силу 25 мая 2018 г.

Предшественником GDPR в Европейском Союзе была Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. «О защите физических лиц при обработке персональных данных и о

свободном обращении таких данных». После принятия GDPR права субъектов ПДн существенно расширились, а обязанности операторов и штрафы за их неисполнение существенно возросли.

Определение ПДн в GDPR мало отличается от определения принятого в Конвенции Совета Европы и от аналогичного определения в отечественном 152-ФЗ: под персональными данными в рамках GDPR понимается любая информация, относящаяся к идентифицированному или идентифицируемому лицу (субъекту персональных данных). Под идентифицируемым лицом понимается то лицо, которое может быть идентифицировано, прямо или косвенно, в частности с использованием таких идентификаторов, как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или при помощи одного или нескольких факторов, специфичных для физического, физиологического, генетического, умственного, экономического, культурного или социального статуса этого лица. Таким образом, под определение ПДн попадают не только привычные нам характеристики, но и IP-адрес, установленные пользователю cookie-идентификаторы, данные о геолокации пользователя и иные технические атрибуты.

Новым важным термином в GDPR является «профилирование» (англ. profiling), под которым понимается любая форма автоматизированной обработки персональных данных в целях оценки определенных аспектов личности, в частности для анализа или предсказания работоспособности человека, его материального положения, здоровья, личных предпочтений, интересов, поведения, местоположения или передвижений.

Зона действия норм GDPR распространяется на всех операторов, которые обрабатывают ПДн граждан ЕС и иных граждан, находящихся на территории ЕС. При этом оператор может не иметь представительства на территории ЕС, а его автоматизированные системы могут также находиться за пределами ЕС. Примеры, касающиеся операторов-компаний из РФ:

- российский банк должен соответствовать нормам GDPR при обработке данных своих клиентов-граждан РФ при их нахождении на территории ЕС;
- онлайн-магазин с регистрацией в РФ, предоставляющий услуги/товары в том числе гражданам ЕС, использующий cookie-идентификаторы и/или аналитику поведения пользователей на своем сайте с интерфейсом на языках ЕС, также подпадает под действие норм GDPR;
- дочерняя структура российской компании, ведущая деятельность на территории ЕС.

Основой норм GDPR являются шесть базовых принципов:

- законность, справедливость и прозрачность обработки – соответствие обработки ПДн законодательству, выработка и следование публично до-

ступной политике по работе с персональными данными (так называемый privacy policy);

- ограничение целей обработки – обработка ПДн осуществляется для определенных, четко выраженных целей и не дольше, чем того требует достижение указанных целей;
- минимизация данных – обработка ровно такого объема ПДн, который требуется для достижения целей обработки;
- точность – обрабатываемые ПДн точны и верны, в противном случае субъект может потребовать удалить или откорректировать неверные ПДн;
- ограничение на хранение – после достижения цели обработки данные удаляются;
- целостность и конфиденциальность – обработка ПДн ведется безопасно, данные защищаются от несанкционированного доступа, случайного или намеренного удаления, утери, повреждения, с применением соответствующих технических и организационных мер.

Документ не дает операторам детальных инструкций по защите, предоставляя им свободу выбора мер и техник. Например, следует, где это возможно, шифровать ПДн при хранении, передаче и обработке, а также использовать алгоритмы псевдонимизации. Это ожидаемо снизит потенциальный ущерб в случае утечки, но GDPR не приводит конкретных условий применения этих защитных мер.

Основополагающий принцип в защите информации решение триединой задачи:

Что защищать? – От кого защищать? – Как защищать?

Что защищать? Это предмет защиты: информация, информационные (автоматизированные) системы, критические процессы и т.д.

От кого защищать? Определение источника угроз (злоумышленника).

Как защищать? Требования (нормы), которые определяют меры подлежащие реализации.

При определении мер защиты информации необходимо помнить, что затраты на обеспечение защиты не должны быть больше стоимости предмета защиты (финансово-экономическая целесообразность).

Стоит отметить, что изучение каждого приведённого документа в этом кратком обзоре методических рекомендаций по изучению дисциплины «ИБАС» предполагает изучение в рамках отдельной лекции при детальном рассмотрении.

Рекомендуемая литература: [2, с. 76–97].

Контрольные вопросы для самопроверки

1. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов, принятые в России и за рубежом в области ИБ.

2. Сформулируйте основные положения Закона РФ «Об информации, информатизации и защите информации» Какие ещё российские законодательные акты вы знаете в этой области?

3. Изложите кратко основное содержание руководящих документов Гостехкомиссии России в области защиты от НСД СВТ и АС.

4. Что представляет из себя стандарт ISO/IEC 17799:2005 «Information technology – Security technique s – Code of practice for information security management» (Информационные технологии. Методы обеспечения безопасности)

5. Назовите главную задачу стандартов информационной безопасности.

3.2 Раздел 2. Современное состояние обеспечения информационной безопасности в автоматизированных системах

3.2.1 Тема 3 Основные регуляторы в области ИБ. Обзор некоторых Интернет-ресурсов в помощь к изучению вопросов информационной безопасности

Перечень изучаемых вопросов

1. Основные ключевые регуляторы в области ИБ, их функции, зоны ответственности.
2. Значение использования современных Интернет-ресурсов в области информационной безопасности.

Методические указания к изучению

В данной теме рассмотрены некоторые основные регуляторы в области ИБ. Приведены зоны их ответственности и функции. Рассмотрены следующие регуляторы: ФСБ России, ФСТЭК России, Минкомсвязи России, Роскомнадзор. В нормативных ссылках в данном пособии представлены соответствующие ссылки на официальные сайты рассмотренных регуляторов.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомназор) – уполномоченный орган по защите прав субъектов персональных данных, осуществляет контроль и надзор за соответствием обработки ПДн требованиям законодательства.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) – федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, устанавливает методы и способы защиты в информационных системах не

криптографическими методами, осуществляет контроль выполнения установленных требований.

Федеральная служба безопасности (ФСБ России) – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, устанавливает методы и способы защиты в информационных системах криптографическими методами, осуществляет контроль выполнения установленных требований.

В современных реалиях сложно переоценить значение Интернет-ресурсов в области ИБ.

С помощью этих ресурсов можно найти ответы на любые вопросы, обсудить профессиональные темы и обменяться ссылками с другими пользователями в области ИБ. Блоги – самый понятный ресурс, в рамках которого авторы делятся опытом, знаниями и быстрыми решениями задач. Руководства по языкам программирования, обзоры интересных проектов, можно найти информацию от программистов со всего мира. Можно найти отзыв на разное ПО и понять для чего оно нужно.

В данном УМП приводится краткая характеристика и назначения соответствующих ресурсов. Более подробно по соответствующим ссылкам, можно познакомиться с этими Интернет-ресурсами, размещённым в системе ЭИОС.

Хабр – русскоязычный веб-сайт в формате системы тематических коллективных блогов с элементами новостного сайта, созданный для публикации новостей, аналитических статей, мыслей, связанных с информационными технологиями, бизнесом и интернетом.

Навигатор безопасника – русскоязычный веб-сайт созданный в помощь для директоров по ИБ, руководителей и начальников отдела или службы ИБ, которые ищут ответы на вопросы по созданию, управлению и совершенствованию процессов ИБ на предприятии.

Системный интегратор «Инфосистемы JET». Джет – русскоязычный веб-сайт, который продает свои услуги. Продает: ЦОД, вычислительные комплексы и СХД, сетевые решения, защита информационной безопасности, управление IT-услугами и IT-инфраструктурой, IT-аутсорсинг и техническая поддержка, разработка ПО, внедрение и сопровождение бизнес приложений. Имеют отраслевые решения: специализированные решения и услуги для операторов связи, банки и финансовые организации, государственные организации и силовые структуры.

SecurityLab – русскоязычный веб-сайт, который имеет новостной блок, статьи, обзор программного обеспечения, блоги компаний и блоги людей в сфере информационной безопасности.

Информзащита – является российским системным интегратором в области информационной безопасности, которая оказывают услуги и предлагают эффективные комплексные решения по информационной безопасности.

Ростелеком – российский провайдер цифровых услуг и сервисов. Предоставляет услуги широкополосного доступа в Интернет, интерактивного телевидения, сотовой связи, местной и дальней телефонной связи и др. Занимает лидирующие позиции на российском рынке высокоскоростного доступа в интернет, платного ТВ, хранения и обработки данных, а также кибербезопасности.

Рекомендуется просмотреть соответствующие ресурсы и найти дополнительные источники веб-ресурсов, которые рассматривают проблемы информационной безопасности. Данный обзор в рамках этой темы нельзя считать полным. Он нужен для того, чтобы продемонстрировать обучающимся возможности и размах системных интеграторов, особенно в реалиях импортозамещения и возможности профессионального роста и трудоустройства в крупные компании, связанные с обработкой информации в области безопасности в автоматизированных системах.

Рекомендуемая литература

1. Состав современных профессиональных баз данных (СПБД) и информационных справочных систем (ИСС).

2. Государственные стандарты Актуализированная база ГОСТов, полностью соответствующая каталогу ФГУП «Стандартинформ» https://docplan.ru/

Контрольные вопросы для самопроверки

1. Какие основные методологические документы ФСТЭК России Вы знаете?

2. Какие руководящие документы ФСТЭК России, описывающие классификацию, Вы знаете?

3. Что такое реестры?

4. Какие виды деятельности ФСБ России Вы знаете?

5. Что такое критическая информационная инфраструктура (КИИ)?

6. Что относится к объектам КИИ?

7. Что относится к субъектам КИИ?

3.2.2 Тема 4 Технологии информационной безопасности и техническая защита информации

Перечень изучаемых вопросов

1. Вирус. Антивирус. Песочницы. Общая информация. Стандартные методы антивирусной защиты. Антивирусное ПО.

2. Межсетевые экраны. Общая информация по программной и аппаратной технологии.

3. Криптография. Инфраструктура открытых ключей (PKI).

4. Защита объектов от утечек по техническим каналам. Система контроля управления данными (СКУД).

Методические указания к изучению

Целью этой темы является знакомство студентов с некоторыми технологиями, которые используются в современных системах защиты информации.

Рассмотрим компьютерные вирусы как специальный класс саморепродуцирующихся программ. Рассмотрим средства антивирусной защиты. Антивирусная программа (антивирус) – любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Рассмотрим жизненный цикл вредоносной программы, среды обитания, отличительные свойства программных закладок, среда обитания, этапы программного противоборства, стандартные методы антивирусной защиты, виды антивирусных средств, простейшие организационные меры.

Sandbox или песочница – изолированная среда для запуска программ с целью поиска ошибок или уязвимостей и предотвращения их дальнейшего распространения. Песочница позволяет защитить критически важные системы сети путем эмуляции рабочей среды выделенным набором ресурсов и запуском в ней подозрительной программы или кода.

Как правило, песочницы используют для запуска непроверенного кода из неизвестных источников, как средство проактивной защиты от вредоносного кода, а также для обнаружения и анализа вредоносных программ.

Ещё одной из технологий мы рассмотрим межсетевые экраны.

Межсетевой экран (МЭ) – это специализированный комплекс, называемый также брандмауэром или системой firewall.

Для большинства организаций установка МЭ является необходимым условием обеспечения безопасности внутренней сети.

Рассмотрим функции МЭ, проблемы безопасности МЭ, схемы сетевой защиты на базе МЭ.

Для изучение работы МЭ используется приобретённое ПО компании Ampier «Киберполигон» ViPNet EndPoint Protection.

ViPNet EPP выявляет нарушения безопасности информации и блокирует угрозы с помощью средств защиты:

• Персональный межсетевой экран – выполняет фильтрацию IP-трафика и блокирует нежелательную сетевую активность.

• Контроль приложений – управляет запуском и активностью приложений, а также их доступом к файлам, реестру ОС Windows, процессам и параметрам командной строки других приложений; предотвращает установку и запуск вредоносного программного обеспечения.

• Обнаружение и предотвращение вторжений – обнаруживает различные сетевые угрозы и блокирует их. ViPNet EPP применяется для защиты отдельных компонентов информационной инфраструктуры организаций – персональных компьютеров пользователей и корпоративных серверов.

На лабораторных занятиях возможно изучить основные режимы работы данного программного продукта, используемого в качестве межсетевого экрана:

Полная блокировка трафика – блокируются любые входящие и исходящие соединения, кроме локального трафика. Компьютер не взаимодействует с внешними сетями.

Публичная сеть – режим рекомендуется использовать при подключении к общественной сети. Режим с максимальной степенью защиты, определяемой корпоративными правилами безопасности.

Частная сеть – режим рекомендуется использовать при подключении к частной сети, например, из дома. Степень защиты определяется корпоративными правилами безопасности. Дополнительно, для учета особенностей фильтрации трафика на компьютере, администратор ViPNet EPP может создавать локальные фильтры.

Защищенная сеть – режим рекомендуется использовать при подключении к частной сети с низким уровнем угроз безопасности внутри периметра сети. Степень защиты определяется только локальными фильтрами, которые может создавать администратор ViPNet EPP.

Отключен – персональный межсетевой экран отключен и не влияет на трафик.

По 3 учебному вопросу в данном методическом указании рассмотрены некоторые криптографические шифры и технология инфраструктуры открытых ключей – это набор служб и сервисов для издания, хранения, обновления и отзыва цифрового сертификата открытого ключа подписи. Изучение было ограничено материалом, который применялся в рамках виртуального программного материала компании DokiSun по следующим разделам:

– Электронная подпись (схема).

– Инфраструктура открытых ключей.

– Гост р 34.11-2012.

– Алгоритм шифрования DES.

– Методы перестановки.
– Шифр Цезаря.
– Метод гаммирования.
– Пропорциональное шифрование.
– Роторная шифровальная машина.
– Хеширование MD5, SHA1.
– RSA.

По четвертому учебному вопросу в данном методическом указании частично приведен теоретический материал по Защите объектов от утечек по техническим каналам и СКУД в рамках применения приведен материал по Функциональности виртуального тренажёра DokiSun:

- Свободное перемещение по виртуальной территории с офисом и складом (свободное условно, так как на проходных точках необходимо применять специальные ключи или карты доступа для прохождения через них).
- Взаимодействие с устройствами СКУД:

– использование различных вариантов ключей и карточек на различных считывателях СКУД Proximity карт, Touch Memory, биометрического терминала;

– использование биометрических данных лица и отпечатков пальцев на биометрическом терминале;

– распознавание автомобильных номеров посредством IP камеры и управление шлагбаумом на парковке;

– настройка и управление центральными устройствами СКУД – контроллерами отдельной охранной комнате с возможностью ограничения к ней доступа.

Изучение визуально-оптических и электрических каналов утечки информации

Теоретический материал

Техническим каналом утечки информации (рисунок 1) называется совокупность источника конфиденциальной информации, среды распространения и средства технической разведки.

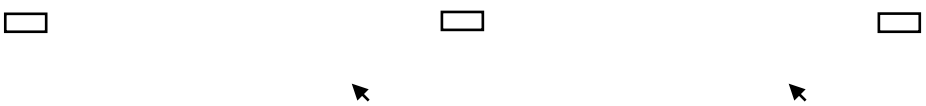

Рисунок 1 – Технический канал утечки информации

Каналы утечки информации можно классифицировать по физическим принципам на следующие группы:

- акустический (прямой, виброакустический, акустоэлектрический, акустооптический, параметрический);
- материально-вещественный (хищение, копирование, ознакомление);
- визуально-оптический (наблюдение, съемка);
- электромагнитный (электрический, индукционный, параметрический).

Информация – любые сведения (сообщения, данные) независимо от формы их представления.

Утечка информации может происходить в трёх формах:

1. Разглашение информации;
2. Реализация технического канала утечки информации (перехват информации с использованием технических средств разведки);
3. Несанкционированный доступ к информации.

Под **утечкой информации** подразумевают неправомерный доступ к информации.

Защищаемая информация – информация, которая является предметом собственности и подлежит защите в соответствие с требованиями нормативных документов или требованиями, устанавливаемыми собственниками информации.

Обработка информации – совокупность различных действий (операций) сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения информации.

Различают основные и вспомогательные технические средства, и системы.

Под основными техническими средства и системами (ОТСС) понимают технические средства передачи, обработки, хранения и отображения защищаемой информации:

- средства вычислительной техники (СВТ);
- средства изготовления и размножения документов;
- системы внутренней автоматической телефонной станцией;
- аппаратура звукоусиления, звукозаписи, звуковоспроизведения;
- технические средства автоматизированных систем управления;
- иные технические средства.

Под вспомогательными техническими средствами и системами (ВТСС) понимают любые технические средства, которые не обрабатывают защищаемую информацию, но находятся в одном и том же помещении с ОТСС:

- системы и средства охранной и пожарной сигнализации;
- системы оповещения и сигнализации;
- контрольно-измерительная аппаратура;

- системы и средства кондиционирования;
- абонентские громкоговорители;
- радиоприёмники;
- телевизоры;
- иные технические средства.

Речевой сигнал – сложный акустический сигнал, основная энергия которого сосредоточена в диапазон частот 170–6000 Гц.

Акустические сигналы – продольные механические волны. Акустическое поле представляет собой пространство, в котором распространяются акустические волны. Звук представляет собой колебания в упругой среде. Частоты акустических колебаний 20–20000 Гц называются звуковыми.

В закрытых помещениях звуковые волны многократно отражаются от ограждающих поверхностей, в результате чего создается сложная картина звукового поля. Законы распределения характеристик звукового поля в данной ситуации определяются не только свойствами источника звука, но и другими факторами – геометрией помещения; способностью стен, потолка и пола поглощать и отражать звуковую энергию. Поэтому звуковые поля в закрытом помещении и в свободном пространстве имеют различные структуры.

Если в свободном пространстве интенсивность звука определяется потоком энергии в направлении распространения волны, то в помещении результирующий поток энергии имеет две составляющие – прямой поток и отраженный (иногда многократно) поток. Звуковой фон в помещении образуют шумы, которые проникают в помещение от различных посторонних и внутренних источников. Из смежных помещений проникают шумы из-за звукопроводности строительных конструкций, ограждающих помещение. Шумы вибрационного происхождения образуются от работающих в здании машин и механизмов. Системы кондиционирования и вентиляции создают внутренние шумы, к которым можно отнести также шумы технологического оборудования (например, шумы вентиляторов компьютеров и других электронных устройств).

Звукопоглощающие материалы бывают сплошными и пористыми. По назначению они подразделяются на:

- стеновые;
- облицовочные;
- для драпировки;
- специальные (мембранные и резонаторные конструкции).

Сплошные материалы. Это в основном твердые материалы (бетон, кирпич, мрамор и т. п.), имеющие акустическое сопротивление существенно больше сопротивления воздуха. Их коэффициенты поглощения очень малы, не более 0,05. Из мягких сплошных материалов в качестве облицовки применяется плотная резина, коэффициент поглощения которой находится в пределах 0,1.

Пористые материалы. К ним относятся штукатурки, облицовочные плиты с перфорацией и без нее, портьеры, ковры и т. п. Они применяются только для облицовки и драпировки. За ними вплотную или на некотором расстоянии располагаются ограждающие конструкции, имеющие сплошную структуру (перекрытия, стены). При воздействии на пористые материалы звуковых волн следует учитывать отражение звука, как от лицевой поверхности, так и от тыльной с учетом поглощения звука в материале.

Резонансные (мембранные и перфорированные) конструкции. Резонансными звукопоглотителями могут служить тонкие перегородки из сплошных материалов Звукопоглощение обусловлено потерей энергии на трение и максимально при резонансе.

Мембранные конструкции представляют собой деревянные рамы с прикрепленными тонкими листами фанеры, пластмассы, полимерной пленки и т. п. Воздушный зазор между слоем и стеной иногда заполняют рыхлым пористым материалом. Перфорированные звукопоглотители представляют собой пористоколебательные системы. Они содержат слой мягкого пористого материала, прикрепленного к стене и покрытого перфорированной пластиной.

Виброакустический канал (рисунок 2)

Воздействие акустических волн на поверхность твердого тела приводит к возникновению в нем вибрационных колебаний в результате виброакустического преобразования. Эти колебания, распространяющиеся в твердой среде, могут быть перехвачены специальными средствами разведки, а речевая информация, содержащаяся в акустическом поле, при определенных условиях может быть восстановлена. С этой целью используют специальные устройства, преобразующие вибрационные колебания в электрические сигналы, соответствующие звуковым частотам. Такие устройства называются вибродатчиками.

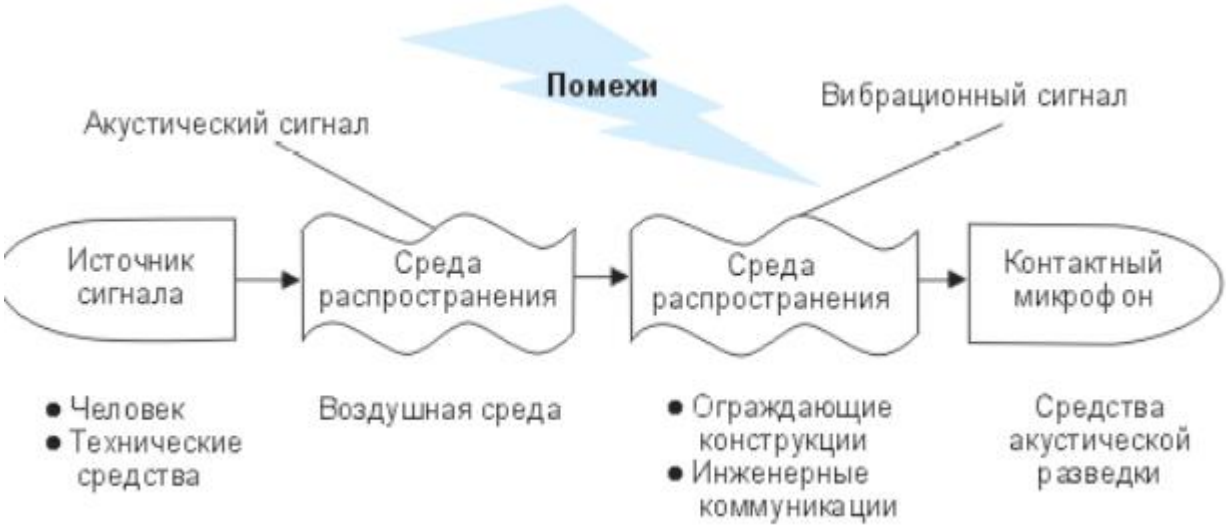

Рисунок 2 – ТКУИ виброакустический

Необходимо отметить, что чем тверже материал преграды на пути распространения акустических колебаний, тем лучше он передает вибрации, вызываемые ими. Поэтому, если стена помещения сделана из гипсолита, сухой штукатурки и т. п., необходимо вбить в нее металлический предмет (можно использовать обычный крупный гвоздь) и крепить датчик стетоскопа непосредственно к нему.

В качестве звукопровода можно использовать трубы водоснабжения, канализации, батареи отопления и т. д. Крепление вибродатчиков к элементам конструкции, по которой распространяются вибрации, может осуществляться с помощью специальных мастик, клеевых составов, магнитов и т. д.

На качество приема вибросигналов кроме свойств вибродатчика и материала твердой среды влияют ее толщина, а также уровни фоновых акустических шумов в помещении и вибраций в твердой среде.

Визуально-оптический канал утечки информации образуется вследствие получения информации путем применения различных оптических приборов, позволяющих уменьшить величину порогового контраста и увеличить контраст объекта на окружающем фоне.

С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты (энергетические ограничения);
- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;
- осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона.

Технические средства приема, обработки, хранения и передачи информации (ТСПИ) – это технические средства, непосредственно обрабатывающие конфиденциальную информацию. К ним относятся: электронно-вычислительная техника, АТС для ведения секретных переговоров, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т. д.

Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (ОТСС).

Наряду с ТСПИ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и которые могут находиться в зоне электромагнитного поля, создаваемого ТСПИ. Такие технические средства и системы называются **вспомогательными техническими средствами и системами (ВТСС)**. К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, средства и системы кондиционирования, электрификации, радиофикации, электробытовые приборы и т. д.

Электрический канал утечки информации возникает за счет:

− наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;

− просачивания информационных сигналов в линии электропитания и цепи заземления ТСПИ;

− использования закладных устройств.

Наводки (токи и напряжения) в токопроводящих элементах обусловлены электромагнитным излучением ТСПИ (в том числе, и их соединительными линиями), а также емкостными и индуктивными связями между ними. Соединительные линии ВТСС или посторонние проводники являются как бы случайными антеннами, при гальваническом подключении к которым средства разведки ПЭМИН возможен перехват наведенных в них информационных сигналов (рисунок 3).

Рисунок 3 – Перехват наведенных электромагнитных излучений ТСПИ с посторонних проводников (инженерных коммуникаций)

Для защиты от утечки информации по электрическому каналу из пассивных способов применяют фильтрацию, ограничение опасных сигналов, защит-

ное отключение, а также экранирование линий, выходящих за пределы контролируемой зоны с заземлением экранирующей оболочки.

Активным способом защиты является линейное зашумление. Системы линейного зашумления (СЛЗ) применяются для зашумления информационных сигналов в кабелях и проводах, выходящих за пределы контролируемой зоны, в следующих случаях:

− при недостаточных уровнях переходных затуханий между влияющими и подверженными влиянию кабелями и соединительными линиями;

− при воздействии на цепи, провода и устройства вспомогательной аппаратуры низкочастотных электромагнитных полей основной аппаратуры;

при наличии электроакустических преобразований во вспомогательной аппаратуре.

Рекомендуемая литература: [1, с. 85–95, 72–77]; [2, с. 193–216, 98–120, 137–141].

Контрольные вопросы для самопроверки

1. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютерными вирусами.
2. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.
3. Охарактеризуйте известные вам основные классы антивирусных программ. В чём смысл комплексного применения нескольких программ?
4. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.
5. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?
6. Какие задачи призван решить МЭ?
7. Перечислите основных производителей МЭ.
8. Для чего используется категорирование межсетевых экранов?
9. Что такое удостоверяющий цент?
10. Hash-значение, что такое?
11. В чём смысл симметричного и асимметричного шифрования?
12. В чём преимущества и недостатки асимметричного и асимметричного шифрования?
13. Как расшифровывается PKI?

3.2.3 Тема 5 Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire»

Перечень изучаемых вопросов

1. Мониторинг и реагирование на инциденты ИБ

2. Учебно-тренировочная платформа Ampire

Методические указания к изучению

Целью изучения этой темы является знакомство студентов с некоторыми трендами, тенденциями, которые позволяют повысить эффективную работу в области ИБ. Это связано с тем, что сейчас сменяется фокус обеспечения ИБ компаний с предотвращения атаки на её раннее обнаружение. В первом вопросе рассмотрим, с чем связано появление адаптивного мониторинга. Рассмотрим историческое развитие.

Первый этап – реактивная обработка. Ручная реакция на инциденты.

Второй этап – инструментальная обработка, которая содержит использование неспециализированных инструментов и технологий.

Третий этап – интегрированная система включает в себя применение специализированных средств, частичная интеграция с различными системами.

Четвёртый этап: стратегическая интеграция – включает в себя тесную интеграцию с ИС компании.

Пятый этап – динамический анализ предполагает наличие АС, которая использует корреляционный анализ, для обнаружения инцидентов ИБ и возможность анализа базы инцидентов.

Шестой этап – продвинутая аналитика подразумевает под собой раннее обнаружение атак различного рода при помощи исторического и поведенческого анализа.

В рамках первого учебного вопроса введены основные определения:

Событие ИБ – любое зафиксированное явление в системе или сети.

Инцидент ИБ – нарушение или угроза нарушения ИБ компании.

Реагирование на инцидент ИБ – структурированная совокупность действий, направленная на установление деталей инцидента, минимизацию ущерба от инцидента и предотвращение повторения инцидента ИБ.

Цели реагирования:

Минимизация ущерба.

Восстановление рабочего состояния ИС.

Недопущение аналогичных инцидентов в будущем.

При анализе инцидента нужно:

– Определить источник атаки.

– Определить какие уязвимости и ПО использовались.

– Определить атакуемые системы.

– Определить на какой стадии находится атака.

– Определить ущерб и др. характеристики атаки.

Киберполигон – это программа, которая имитирует IT-инфраструктуру целого ряда предприятий из ключевых отраслей экономики. Создание такой

площадки предусмотрено федеральным проектом «Информационная безопасность» в рамках национальной программы «Цифровая экономика».

Практическое использование Киберполигона позволяет выполнять следующие задачи, стоящие перед нацпроектом:

– обеспечение подготовки высококвалифицированных кадров для цифровой экономики;

– обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства.

Главная его задача – это моделирование действий нарушителя путём развития компьютерной атаки и исследование компьютерных инцидентов на инфраструктуре предприятия. Киберполигон позволяет проводить учения и тренировки, в ходе которых IT-специалисты смогут отрабатывать ответные действия на случай кибератак. Для реагирования на компьютерные инциденты, обеспечение безопасности в компьютерных сетях в ходе киберучений создаются команды мониторинга и защиты (реагирования). Основная задача команд – действия по защите от несанкционированной деятельности в информационных сетях, включая мониторинг, обнаружение, анализ, реагирование и восстановление.

Существует множество терминов, которые используются для обозначения команд экспертов по кибербезопасности, выполняющих задачи по защите ИС, например, команда SOC (Security Operations Center, или Центр обеспечения безопасности). Киберспециалисты в команде SOC вооружены современными технологиями обнаружения инцидентов в режиме реального времени, анализа вторжений, подготовки отчётов о состоянии безопасности и киберинцидентах.

Самое трудоемкое в работе команды SOC – это осуществление непрерывного контроля за безопасностью организации. Оценить потенциал команды в «боевой» обстановке на ИС организации, наверное, не лучшее решение, но провести учения и оценить свой потенциал позволит киберполигон.

Оборудование для Центра обеспечения безопасности включает системы контроля доступа, системы обнаружения вторжений, консоли и различное специализированное программное обеспечение, которое в том числе внедрено в обучающий программный комплекс «Ampire».

В используемый шаблон входят следующие сегменты:

– сеть Интернет;

– внешний периметр организации;

– корпоративный центр обработки данных;

– пользовательский отдел «Разработчики»;

– пользовательский отдела «Пользователи»;

– АСУ ТП.

А также в сценарий могут быть включены комплексы, осуществляющие сбор, накопление, систематизацию и анализ информации, которая поступает в данную систему через средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Практические занятия на цифровом двойнике реальной инфраструктуры проводятся с использованием симуляции сети с ИТ и SCADA-сегментами

Рекомендуемая литература

1. Состав современных профессиональных баз данных (СПБД) и информационных справочных систем (ИСС).

2. Государственные стандарты Актуализированная база ГОСТов, полностью соответствующая каталогу ФГУП «Стандартинформ» https://docplan.ru/

Контрольные вопросы для самопроверки

1. Для чего предназначен киберполигон?
2. Как называется программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак, разработанный АО «Перспективный мониторинг»?
3. Какие категории пользователей может быть в ПК «Ampire»?
4. Какие команды могут принять участие в киберучениях на базе ПК«Ampire»? Укажите их задачи.

Какой файл и в каком формате необходимо добавить в карточку инцидента ИБ?

3.2.4 Тема 6 Введение в изучение среды моделирования «Киберполигон» для исследования атак с использованием средств обнаружения вторжений

Перечень изучаемых вопросов

1. Назначение, состав и основные возможности программного комплекса «Ampire».

2. Обнаружение признаков атак на сервисы на уровне хоста, на уровне сети.

Методические указания к изучению

Задачами программного комплекса «Киберполигон» являются:

– отработка навыков анализа событий ИБ;

– отработка навыков управления инцидентами ИБ (выявление, реагирование, анализ последствий);

– отработка навыков организации реагирования на инциденты ИБ;

– отработка навыков по устранению уязвимостей информационных системах общего и специального назначения;

– отработка навыков по оценке защищенности элементов информационных сетей;

– отработка взаимодействия между подразделениями;

отработка превентивных мер по предупреждению компьютерных атак.

В ходе выполнения практических занятий на ПК Ampire обучаемые получают навыки:

– мониторинга и обнаружения компьютерных атак, направленных на элементы ИС организации;

– работы со специальным программным обеспечением для обнаружения и анализа событий ИБ;

– подготовки предложений по нейтрализации выявленных недостатков безопасности в ИС организации;

– локализации объектов атаки и внесения изменений в элементы ИС организации для нейтрализации выявленных угроз;

– настройки и корректировки средств защиты информации для повышения уровня защищенности ИС организации.

Киберучения – это процесс моделирования целевых компьютерных атак на некую ИТ-инфраструктуру с акцентом в сторону отработки навыков защиты (концепция Blue Team), изучения принципов эксплуатации уязвимостей нарушителем (концепция Red Team). В ходе киберучений осуществляются:

– анализ событий ИБ; регистрация и расследование инцидентов ИБ;

– устранение причин успешного выполнения компьютерных атак;

– командное взаимодействие.

В основе киберучений лежит шаблон некоторой ИС, на которую проводится полностью автоматизированная учебная компьютерная атака, моделирующая действие внешнего или внутреннего нарушителя. Задачи по анализу событий ИБ и заведению карточек инцидентов ИБ возлагаются на участников группы мониторинга, ликвидация последствий инцидентов ИБ – на группу реагирования. Процесс киберучений выполнен единообразно для всех шаблонов и сценариев, поставляемых вместе с комплексом.

В ПК «Ampire» каждый пользователь принадлежит к одной из трёх категорий: администратор, преподаватель или обучаемый.

Для функционирования ПК «Ampire» использовано различное программное обеспечение сторонних производителей, в том числе: ОС Debian 9.0, один из дистрибутивов операционной системы Linux с большим количеством пакетов; Docker 17.10.0, программное обеспечение с открытым исходным кодом, применяемое для разработки, тестирования, доставки и запуска веб приложений в средах с поддержкой контейнеризации. Данное ПО необходимо для эффективного использования системы и ресурсов, быстрого развертывания готовых программных продуктов, а также для их масштабирования и переноса в другие среды с гарантированным сохранением стабильной работы; PostgreSQL – свободно распространяемая объектно-реляционная система управления базами данных; Nginx, HTTP-сервер и IMAP/POP3 прокси-сервер

для UNIX-подобных платформ; Gunicorn – автономный веб-сервер с обширной функциональностью, поддерживает различные фреймворки (облегчающие разработку и объединение разных компонентов большого программного проекта) и адаптеры; Daphne – это удобный менеджер задач для Windows; Vue.js – Javascript фреймворк для создания пользовательских интерфейсов; Python 3.6.5 – высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода; pip 19.1 – система управления пакетами, написанными на Python. В работе комплекса используются различные дополнительные пакеты pip, представленные на рисунке 4.

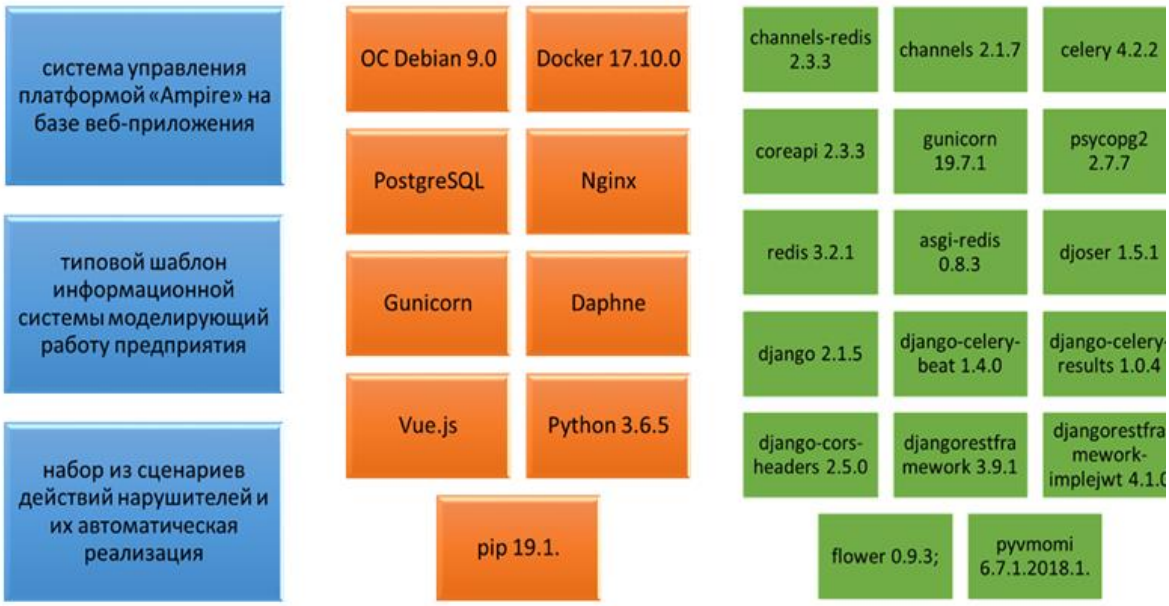

Рисунок 4 – Структура комплекса

Для проведения занятий на учебном комплексе «Ampire» необходимо подготовить рабочие места для пользователей (стационарные компьютеры или ноутбуки). Системные требования к рабочим местам: процессор Core i5 или выше; оперативная память не менее 4 Гб; жесткий диск не менее 100 Гб; операционная система Windows 8, 8.1, 10. Все рабочие места обучаемых должны быть подключены к комплексу через локальную сеть (при удалённом подключении через VPN, организованное администратором). Все взаимодействия с ПК «Ampire» осуществляется через браузер, рекомендуется использовать Google Chrome 78 или выше.

При проведении занятия преподавателю доступна возможность управления виртуальными нарушителями (запуск сценария атаки, остановка, выполнение отдельных этапов), формирование команд участников: группы мониторинга и защиты (реагирования), просматривать и оценивать создаваемые обучаемыми карточки инцидентов ИБ, а также Создание групп необходимо для минимиза-

ции времени реагирования на инцидент, качественного проведения анализа привлеченными в состав группы участниками, разбора причин инцидента, а также выработки мер по недопущению повторных инцидентов.

В процессе тренировки преподаватель может в онлайн-режиме отслеживать статусы заложенных в шаблон уязвимостей, корректность работы всех узлов ИС, на которой проходит тренировка, перечень и детали по каждой карточке инцидента ИБ. Обучаемый имеет доступ к встроенным в шаблон ИС средствам обнаружения компьютерных атак, а также дополнительным системам защиты информации, характерных для выбранной тренировки. Обучаемый, выполняя роль в группе мониторинга, имеет возможность создавать карточки инцидентов ИБ и получать по ним обратную связь. При участии в группе реагирования пользователю доступна возможность непосредственного подключения к узлам ИС, используемого шаблона (рисунок 5), для проведения детального анализа инцидента ИБ и внесения изменений для устранения уязвимостей информационной безопасности.

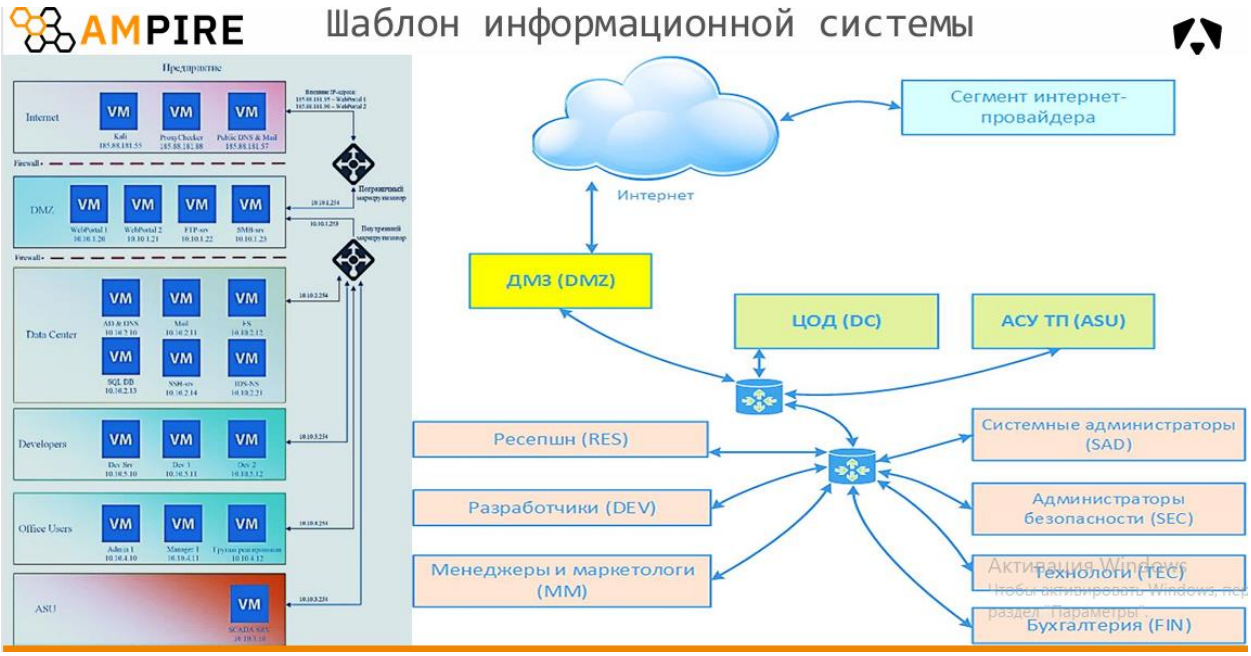

Рисунок 5 – Шаблон ИС

В основе киберучений лежит шаблон некоторой ИС (рисунок 5), на которую проводится полностью автоматизированная учебная компьютерная атака, моделирующая действие либо внешнего, либо внутреннего нарушителей. Задачи по анализу событий ИБ и заведения карточек инцидентов ИБ возлагаются на участников группы мониторинга, а расследование инцидентов ИБ и устранение уязвимостей – на группу реагирования. Процесс киберучений выполнен единообразно для всех шаблонов и сценариев, поставляемых вместе с комплексом.

Основные шаги следующие:

1. Преподаватель создает тренировку на базе имеющегося шаблона, указывая на соответствующий сценарий, моделирующий действия виртуального нарушителя.

2. После создания тренировки преподаватель активирует учебную компьютерную атаку на виртуальную инфраструктуру.

3. Действия виртуального нарушителя регистрируются различными системами обнаружения вторжений (СОВ) на уровне сети и на уровне конечных узлов.

4. Участники группы мониторинга проводят анализ зафиксированных событий при помощи СОВ и заводят карточки инцидентов ИБ.

5. Участники группы реагирования проводят анализ полученных карточек инцидентов ИБ, подключаются к отдельным узлам ИС тренировки и устраняют имеющиеся в них уязвимости. Созданные команды должна обеспечить: понятную, эффективную, динамичную процедуру реагирования на инциденты; координацию и управление всеми привлеченными для устранения инцидента экспертами; оперативный сбор актуальной информации с оборудования; оперативный анализ полученной информации и формирование рекомендаций; формирование предложений в результате разбора и анализа инцидента; реагирование на произошедший инцидент и устранение последствий.

Тренировка заканчивается, когда устранены все уязвимости в составе активной тренировки или время тренировки закончилось. Участники группы мониторинга действуют независимо друг от друга. Основными их задачами являются: анализ событий ИБ; заведение карточек инцидентов ИБ; описание вектора атаки виртуального нарушителя. Участники группы защиты (реагирования) действуют коллективно. Для этого среди них назначается старший группы, который распределяет получаемые от группы мониторинга карточки инцидентов ИБ.

Основными их задачами являются: расследование инцидентов ИБ; устранение уязвимостей, которые намеренно внесены в шаблон, используемый для тренировки. Группа защиты преследует цели объединить всех участников, каждый из которых несет ответственность за определенную область в этом процессе, для эффективного взаимодействия, управления процессом и оперативного решения возникающих в ходе разбора инцидента вопросов и проблем. Руководитель (лидер) группы: организует и направляет работу группы; на время расследования инцидента является руководителем для всех привлеченных участников группы; имеет полномочия по привлечению необходимых экспертов в группу на время расследования инцидентов; осуществляет контроль и проверку исполнения решений, принятых в рамках реагирования на инцидент. Участник группы защиты, назначенный ответственным за выполнение того или иного этапа в рамках реагирования на инцидент, вправе привлечь к выполнению задач любого участника группы

В ходе тренировки преподаватель формирует команду мониторинга.

Задача команды выполнять мониторинг, искать и анализировать вторжения в режиме реального времени. При этом используются современные реше-

ния по обнаружению и предотвращению компьютерных атак, в частности, сетевой сенсор системы обнаружения атак ViPNet IDS NS.

Порядок работы участника группы мониторинга состоит из нескольких этапов:

1. Подготовить к тренировке АРМ (выполняется в ходе идентификации и аутентификации в ПК «Ampire» и подключения к тренировке).

2. Подключиться к средствам обнаружения компьютерных атак (вторжений) и вредоносного ПО.

3. Провести анализ сетевого трафика. Мониторинг угроз, анализ событий и выявить инциденты информационной безопасности.

4. Создать карточки ИБ.

Основные определения для работы в группе мониторинга и использования СОВ приведены ниже.

• **Вторжение (атака)** – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам

• **Система обнаружения вторжений (СОВ)** – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней

Англоязычный термин – ***Intrusion Detection System (IDS)***

• **Администратор СОВ** – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию СОВ.

• **Анализатор СОВ** – программный или программно-технический компонент СОВ, предназначенный для сбора информации от сенсоров (датчиков) СОВ, ее итогового анализа на предмет обнаружения вторжения (атаки) на контролируемую ИС

• **База решающих правил** - составная часть СОВ, содержащая информацию о вторжениях (сигнатуры), на основе которой СОВ принимает решение о наличии вторжения (атаки)

• **Данные СОВ** – данные, собранные или созданные СОВ в результате выполнения своих функций

• **Датчик (сенсор)** СОВ – программный или программно-технический компонент СОВ, предназначенный для сбора и первичного анализа информации (данных) о событиях в контролируемой ИС, а также – передачи этой информации (данных) анализатору СОВ.

СОВ включает следующие подсистемы:

– сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;

– подсистему анализа, предназначенную для выявления атак и подозрительных действий;

– хранилище, обеспечивающее накопление первичных событий и результатов анализа;

– подсистему реагирования на выявленные вторжения;

– консоль управления, позволяющую конфигурировать и наблюдать за состоянием защищаемой системы, а также просматривать выявленные подсистемой анализа инциденты

Обнаружение признаков атак на уровне сети

Угадывание паролей; репликационный код; взлом паролей; использование известных уязвимых мест; отключение/обход систем аудита; воровство данных; back doors (специальные входы в программу, возникающие из-за ошибок при ее написании или оставленные программистами для отладки); использование снифферов и sweepers (систем контроля содержимого); использование программ диагностики сети для получения необходимых данных; использование автоматизированных сканеров уязвимостей; подмена данных в IP-пакетах; атаки типа «отказ в обслуживании» (DoS); атаки на Web-серверы; (CGI-скрипты) технологии скрытого сканирования; распределенные средства атаки.

На рисунке ниже приведена классификация систем обнаружения атак (рисунок 6).

Рисунок 6 – Классификация систем обнаружения атак

Принцип работы системы обнаружения вторжений (на примере ViPNet IDS NS) состоит из следующих шагов и приведён на схеме рисунка 7:

1. Злоумышленник начинает реализацию сетевой атаки на локальную сеть.

2. Вредоносные пакеты проходят в защищаемую сеть, поскольку атака проводится в рамках, разрешенных на межсетевом экране соединений.

3. Злоумышленник выполняет удаленный запуск эксплойта на одном из компьютеров защищаемой сети.

4. Устройство дублирования трафика направляет копии вредоносных пакетов на интерфейс захвата ViPNet IDS NS.

5. ViPNet IDS NS обнаруживает угрозу в захваченном пакете сигнатурным методом. В результате срабатывает правило и в журнале регистрируется событие.

6. Выполняется анализ информации о зарегистрированном событии (IP-адреса источников и получателей тип угрозы и другие) на терминале управления в графическом веб-интерфейсе ViPNet IDS NS.

7. Выполняется реагирование на сетевую атаку – на межсетевом экране создается блокирующее правило.

8. Сетевая атака остановлена. Злоумышленник не имеет доступа к узлам защищаемой сети

Рисунок 7 – Принцип работы СОВ

3.2.4.1 Сетевой сенсор системы обнаружения атак программно-аппаратный комплекс ViPNet IDS NS 3

Методы анализа сетевого трафика

Для обнаружения угроз в ViPNet IDS NS выполняется анализ сетевого трафика следующими методами:

- Сигнатурный метод – анализ заголовков протоколов и содержимого сетевых пакетов на основе сигнатурных правил.
- Эвристический метод – отслеживание отклонений параметров сетевого трафика от эталонной модели.
- Malware detection – анализ файлов, передаваемых в сетевом трафике, на наличие вредоносного ПО.

• Анализ служебных полей заголовков протоколов на наличие аномалий (RPC, HTTP, SMTP, FTP, SSH, MODBUS, GTP, SIP, Telnet, TCP, SSL, IMAP, DNS, DNP3, MODBUS, POP), отслеживание попыток сканирования портов и передачи конфиденциальных данных (номеров банковских карт, адресов электронной почты).

•Отслеживание ARP-spoofing – анализ служебных заголовков ARP-пакетов и ведение внутренней ARP-таблицы с целью отслеживания попыток сетевых атак типа ARP-spoofing.

3.2.4.2 Программно-аппаратный комплекс ViPNet TIAS

ViPNet TIAS (Threat Intelligence Analytics System) представляет собой систему интеллектуального анализа угроз безопасности информации, относящихся к атакам.

ViPNet TIAS предназначен для автоматического выявления инцидентов информационной безопасности в информационных системах на основе анализа информации о событиях информационной безопасности, поступающей от источников – сенсоров обнаружения атак (вторжений).

ViPNet TIAS является эффективным инструментом для специалистов, ответственных за обеспечение информационной безопасности, при расследовании выявленных инцидентов и выборе способа реагирования на них.

ViPNet TIAS входит в состав решения ViPNet TDR (Threat detection and response) — системы обнаружения и реагирования на компьютерные атаки.

В ViPNet TDR обнаружение угроз и регистрацию событий информационной безопасности выполняют сенсоры:

• Сетевой сенсор системы обнаружения атак ViPNet IDS NS (далее – сетевой сенсор).

• Система обнаружения вторжений ViPNet IDS HS (далее – узловой сенсор).

Более подробно с работой данных программно-аппаратных комплексов можно ознакомиться, изучив руководство администратора (см. список литературы). Данное руководство будет размещено в среде ЭИОС.

Рекомендуемая литература (руководства по эксплуатации, интернет-источники)

1. Состав современных профессиональных баз данных (СПБД) и информационных справочных систем (ИСС).

2. Государственные стандарты Актуализированная база ГОСТов, полностью соответствующая каталогу ФГУП «Стандартинформ» https://docplan.ru/

Контрольные вопросы для самопроверки

1. Для чего предназначен комплекс программных и программно-технических средств ViPNet IDS?

2. До какого класса защищённости комплекс ViPNet IDS может использоваться в информационных системах персональных данных, в государственных информационных системах?

3. Из каких компонентов состоит комплекс ViPNet IDS?

4. Что понимается под базой правил, системными правилами и где они формируются?

5. Какое принципиальное отличие мониторинга от анализа событий и инцидентов информационной безопасности КИИ?

6. Какие уровни критичности атак различает ViPNet IDS?

7. В каких исполнениях выпускается ViPNet IDS NS?

8. Какие способы подключения ViPNet IDS NS возможны в сети организации?

9. Как администратор может осуществлять доступ и управление системой ViPNet IDS?

10. Что входит в состав программного обеспечения сетевого сенсора ViPNet IDS NS?

11. Какие дополнительные возможности предоставляет использование ПАК ViPNet TIAS?

12. Какие сетевые интерфейсы ViPNet IDS NS не нуждаются в настройке IP-адресов?

4. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБО

Лабораторные занятия направлены на углубление знаний и закрепление основных понятий и методов, изучаемых в рамках дисциплины. Основная цель занятий – научиться применять теоретические знания для решения прикладных задач.

Рекомендации к подготовке

1. Изучение лекционного материала и конспектов:

– Перед лабораторными занятиями необходимо проработать соответствующие разделы лекционного материала.

– Рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом лабораторного занятия.

2. Проработка учебной литературы:

– Используйте основные учебники и методические пособия, рекомендованные преподавателем.

– Для глубокого понимания теории рекомендуется обращаться к дополнительной литературе.

3. Подготовка вопросов:

– Составьте список вопросов по материалу, вызвавшему затруднения.

– Обсуждение этих вопросов на лабораторном занятии поможет устранить пробелы в знаниях.

4. Вопросы для самоконтроля:

– Перед каждым занятием рекомендуется проверять себя с помощью вопросов для самоконтроля из методических указаний к лекционным занятиям. Это позволит оценить уровень своей подготовки.

В этом разделе приведены общие рекомендации. Информация, которая касается тематического плана выполнения лабораторных работ приведена в таблице 1 данного документа. Подробная информация по выполнению лабораторных работ приведена в УМП по выполнению лабораторных работ по дисциплине «Информационная безопасность автоматизированных систем».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

Внеаудиторная самостоятельная работа в рамках данной дисциплины включает в себя:

• подготовку к аудиторным занятиям (лекциям, лабораторным занятиям) и выполнение соответствующих заданий;

• самостоятельную работу над отдельными темами учебной дисциплины в соответствии с тематическим планом;

• подготовку к зачету.

Подготовка к лекционным занятиям:

При подготовке к лекции рекомендуется повторить ранее изученный материал, что дает возможность получить необходимые разъяснения преподавателя непосредственно в ходе занятия. Рекомендуется вести конспект, главное требование к которому быть систематическим, логически связанным, ясным и кратким. По окончанию занятия обязательно в часы самостоятельной подготовки, по возможности в этот же день, повторить изучаемый материал и доработать конспект.

Подготовка к лабораторным занятиям:

Подготовка к лабораторным занятиям предусматривает:

• изучение теоретических положений по изучаемой теме;

• детальную проработку учебного материала, рекомендованной литературы и методической разработки на предстоящее занятие;

Самостоятельная работа над отдельными темами учебной дисциплины:

При организации самостоятельного изучения ряда тем лекционного курса обучаемый работает в соответствии с указаниями, выданными преподавателем. Указания по изучению теоретического материала курса составляются диффе-

ренцированно по каждой теме и включают в себя следующие элементы: название темы; цели и задачи изучения темы; основные вопросы темы; характеристику основных понятий и определений, необходимых обучаемому для усвоения данной темы; список рекомендуемой литературы; наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т. п.; краткие выводы, ориентирующие обучаемого на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить; контрольные вопросы, предназначенные для самопроверки знаний.

Подготовка к зачету

При подготовке к зачету большую роль играют правильно подготовленные заранее записи и конспекты. В этом случае остается лишь повторить пройденный материал, учесть, что было пропущено, восполнить пробелы, закрепить ранее изученный материал.

В ходе самостоятельной подготовки к зачету при анализе имеющегося теоретического и лабораторного материала студенту также рекомендуется проводить постановку различного рода задач по изучаемой теме, что поможет в дальнейшем выявлять критерии принятия тех или иных решений, причины совершения определенного рода ошибок. При ответе на вопросы, поставленные в ходе самостоятельной подготовки, обучающийся вырабатывает в себе способность логически мыслить, искать в анализе событий причинно-следственные связи.

6. КОНТРОЛЬ И АТТЕСТАЦИЯ

К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

– тестовые задания закрытого и открытого типов.

Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно-корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи

Система оценок / Критерий	2	3	4	5
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

Задание открытого и закрытого типа приведены в ФОС (приложении к рабочему модулю).

Типовые контрольные задания и иные материалы, необходимые для оценки результатов освоения дисциплин модуля (в том числе в процессе освоения), а также методические материалы, определяющие процедуры этой оценки приводятся в приложении к рабочей программе модуля. Оценивание результатов обучения проводится с применением электронного обучения, дистанционных образовательных технологий.

7. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература

1. Леонтьев, А. С. Защита информации: учеб. пособие / А. С. Леонтьев. – Москва: РТУ МИРЭА, 2021. – 79 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/182491 (дата обращения: 18.08.2024). – Текст : электронный.

2. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. – 5-е изд., стер. – Санкт-Петербург: Лань, 2023. – 124 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/293009 (дата обращения: 18.08. 2024). – ISBN 978-5-507-46010-6. – Текст : электронный.

3. Краковский, Ю. М. Методы защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – 3-е изд., перераб. – Санкт-Петербург: Лань, 2021. – 236 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/156401 (дата обращения: 18.08.2024). – ISBN 978-5-8114-5632-1. – Текст : электронный.

4. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. – 5-е изд., стер. – Санкт-Петербург: Лань, 2023. – 96 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/288974 (дата обращения: 18.08.2024). – ISBN 978-5-507-45868-4. – Текст : электронный.

5. Технологии обеспечения безопасности информационных систем: учеб. пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 210 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 18.08.2024). – ISBN 978-5-4499- 1671-6. – DOI 10.23681/598988. – Текст : электронный.

Дополнительная литература

6. Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: ЮнитиДана: Закон и право, 2018. – 287 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 18.08.2024). – ISBN 978-5-238-02857-6. – Текст : электронный.

7. Климентьев, К. Е. Введение в защиту компьютерной информации: учеб. пособие / К. Е. Климентьев. – Самара: Самарский университет, 2020. – 183 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-

библиотечная система. – URL: https://e.lanbook.com/book/189043 (дата обращения: 18.08.2024). – ISBN 978-5-7883-1526-3. – Текст : электронный.

8. Горбачев, А. А. Техническая защита информации. Поисковые приборы: учеб. пособие / А. А. Горбачев, С. И. Алешников. – Калининград: БФУ им. И. Канта, 2022. – 148 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/310139 (дата обращения: 18.08.2024). – ISBN 978-5-9971-0696-6. – Текст : электронный.

9. Комплексное обеспечение информационной безопасности автоматизированных систем: учеб. пособие / сост. М. А. Лапина [и др.]. – Ставрополь: СКФУ, 2016. – 242 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/155111 (дата обращения: 25.08.2024). – Текст : электронный.

10. Корниенко, А. А. Система требований к обеспечению безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры: учеб. пособие / А. А. Корниенко, В. С. , А. П. Глухов. – Санкт-Петербург: ПГУПС, 2022. – 63 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/329477 (дата обращения: 25.08.2024). – ISBN 978-5-7641-1837-6. – Текст : электронный.

Учебно-методические пособия, нормативная литература

11. Шилер, А. В. Информационно-аналитическая работа по обеспечению информационной безопасности автоматизированных систем: учеб.-метод. пособие / А. В. Шилер, Е. А. Степанова. – Омск: ОмГУПС, 2023. 21 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/419624 (дата обращения: 25.08.2024). – Текст : электронный.

12. Учебно-методическое пособие по дисциплине «Сетевая безопасность»: учеб.-метод. пособие / сост. А. В. Ванюшина, М. А. Фармаковский. – Москва: МТУСИ, 2021. – 72 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/333782 (дата обращения: 12.08.2024). – Текст : электронный.

13. Назаров, А. Н. Информационная безопасность в сетях общего пользования: учеб.-метод. пособие / А. Н. Назаров, Е. Г. Андрианова. Москва: РТУ МИРЭА, 2023. – 52 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/368963 (дата обращения: 12.08.2024). – ISBN 978-5-7339-1751-1. – Текст : электронный.

14. Киреева, Н. В. Методические рекомендации по выполнению лабораторных работ по дисциплине «Информационная безопасность инфокоммуникационных сетей и систем»: учеб.-метод. пособие / Н. В. Киреева, О. А. Караулова. – Самара: ПГУТИ, 2022. – 40 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/411743 (дата обращения: 12.08.2024). – Текст : электронный.

Локальный электронный методический материал

Наталья Яронимо Великите

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 3,6. Печ. л. 3,1.

Издательство федерального государственного бюджетного образовательного учреждения высшего образования
«Калининградский государственный технический университет»
236022, Калининград, Советский проспект, 1