Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»

А. А. Бабаева

ПРОЕКТИРОВАНИЕ ОТКРЫТЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Учебно-методическое пособие по выполнению лабораторных работ для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент
доцент кафедры информационной безопасности ФГБОУ ВО
«Калининградский государственный технический университет»
А. Г. Жестовский

Бабаева, А. А.
Проектирование открытых систем в защищенном исполнении: учебно-методическое пособие по выполнению лабораторных работ для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем / А. А. Бабаева. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 38 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Проектирование открытых систем в защищенном исполнении» студентами, обучающимися по специальности 10.05.03 Информационная безопасность автоматизированных систем. Учебно-методическое пособие предназначено для приобретения практических навыков проектирования, создания, эксплуатации, открытых систем и обеспечения их безопасности на всех этапах жизненного цикла.

.

Список лит. – 6 наименований.

Пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по выполнению лабораторных работ рекомендовано в качестве локального электронного методического материала для использования в учебном процессе методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 4

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем, изучающих дисциплину «Проектирование информационных систем в защищенном исполнении».

Цель выполнения лабораторных работ - заложить фундамент для решения задач информационной безопасности, научить анализировать угрозы информационной безопасности, научить создавать модель угроз и модель нарушителя с учетом специфики защищенной автоматизированной системы, рассмотреть основные общеметодологические принципы обеспечения информационной безопасности автоматизированных систем.

Лабораторный практикум содержит семь лабораторных работ.

В результате выполнения лабораторных работ ожидается, что студенты сформируют навыки решения задач информационной безопасности открытых систем, научатся анализировать угрозы и уязвимости информационной безопасности открытых систем и проектировать открытые системы в защищенном исполнении.

Лабораторная работа № 1
Описание информационной системы персональных данных

Цель работы: Составить описание ИСПДн, определив назначение, структуру и основные характеристики ИСПДн (вашего объекта).

Ход работы

1. Выбрать ту ИСПДн, информацию о которой сможете найти (с места прохождения практики, знакомые, родители). Либо выбрать абстрактный объект и написать его полное описание, полагаясь на свои знания или сведения доступных источников о структуре и назначении.
2. Указать название объекта, территориальное расположение (важно понимать: находится ли ИСПДн в одном городе/здании/помещении или это комплекс), род деятельности и назначение.
3. Определить структуру и основные характеристики ИСПДн. Для этого необходимо указать следующее:
   1) какие персональные данные обрабатываются в системе;
   2) где располагаются основные компоненты ИСПДн (внутри/снаружи контролируемой зоны);
   3) какие действия с ПД предусмотрены в режиме обработки;
   4) заполнить таблицу 1:

Таблица 1 - Структура и характеристики ИСПДн

Заданные характеристики безопасности персональных данных	
Структура информационной системы	
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	
Режим обработки персональных данных	
Режим разграничения прав доступа пользователей	
Местонахождение технических средств информационной системы	
Дополнительная информация	

5) Определить категорию ПД, обрабатываемых в системе;
6) Показать конфигурация элементов ИСПДн, территориальное расположение ИСПДн относительно контролируемой зоны и структурную организационную схему основных отделов объекта (предприятия);

7) Указать характеристики серверного оборудования, входящего в состав АИС и перечень программного обеспечения, установленного на серверах, где ведется обработка ПД;
8) Указать тип разграничения прав доступа пользователей, заполнить таблицу 2:

Таблица 2 - Матрица доступа

Группа	**Уровень доступа к ПДн**	**Разрешенные действия**	**Сотрудники отдела**
Администратор безопасности	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Сотрудник отдела защиты информации
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Бухгалтера

9) Составить список всех программных и аппаратных средств на объекте и указать информационные ресурсы;
10) Указать основные средства защиты и разграничения доступа в ИСПДн.

Отчет:

Результат выполнения работы необходимо оформить в виде отчета по лабораторной работе и защитить преподавателю. Для успешной защиты необходимо указать ответы на все пункты задания по ходу выполнения работы и уметь ответить на вопросы по теме лабораторной работы.

Пример структурной схемы и описания объекта:

Федеральное государственное бюджетное учреждение «Администрация морских портов балтийского моря». Организационная структура данного предприятия изображена на рисунке 1.

Рисунок 1 - Организационная структура ФГБУ АМПБМ

Информационные ресурсы**:**

- информация о компании;

- информация из государственных органов и органов управления (законы, постановления, налоговые органы);

- схема порта;

- информация для агентских компаний и судовладельцев;

- нормативные документы;

- правила режима в морском пункте пропуска в морском порту Калининград;

- технологическая схема организации пункта пропуска.

Информационная система:
- ОС;
- офисные программы (MS Office);
- 1С «Предприятие» и компоненты для работы ИС;
- КриптоПро;
- БД;
- маршрутизатор;
- антивирусные программы;
- серверы видеонаблюдения.
- маршрутизаторы, коммутаторы cisco.

Лабораторная работа № 2
Определение задач защиты. Выделение основных функций и задач защиты информации

Цель работы: Определить субъекты и объекты защиты на предприятии (организации) и сформировать основные задачи защиты информации.

Основными задачами системы ИБ являются:

- своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;
- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем и сетей с учетом определений ГОСТ Р 50922—96. Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от НСД — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим НСД к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Система защиты информации — совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Современная автоматизированная система (АС) обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты АС можно разбить на следующие группы:

• аппаратные средства — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);

• программное обеспечение — приобретенные программы, исходные, объектные, загрузочные модули; ОС и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

• данные — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;

• персонал — обслуживающий персонал и пользователи.

• объекты системы — пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;

• субъекты системы — активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы. Субъекты могут быть внешними и внутренними

Ход работы

1. Определить объекты системы и указать те, которые являются критически важными.
2. Определить субъекты системы (внешние и внутренние).
3. Определить задачи защиты системы ИБ для объекта и указать: какие компоненты и средства защиты обеспечивают их выполнение на вашем объекте.

Отчет

Результат выполнения работы необходимо оформить в виде отчета по лабораторной работе и защитить преподавателю. Для успешной защиты необходимо указать ответы на все пункты задания по ходу выполнения работы и уметь ответить на вопросы по теме лабораторной работы.

Лабораторная работа № 3

Виды моделей угроз и уязвимостей. Создание модели угроз и уязвимостей для своего объекта

Перед выполнением работы необходимо ознакомиться с интернет ресурсом https://fstec.ru/ документами в разделе «Техническая защита информации»:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2007 год.

Примечание. В связи с утверждением методического документа Методика оценки угроз безопасности информации от 05 февраля 2021 года не применяются для оценки угроз безопасности информации, Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.) и Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007 г.).

Цель работы: создать модель угроз и уязвимостей для своего объекта. Определить вероятность, возможность реализации угроз. Указать актуальность для угроз каждого типа.

Целью реализации угроз является нарушение определенных для объекта реализации угроз характеристик безопасности (таких как, конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта.

Ход работы

1)В соответствии с положениями определить: какие угрозы несут потенциальную опасность нарушения безопасности персональных данных при их обработке в ИСПДн данного типа. Определить исходный уровень защищенности ИСПДн и заполнить таблицу 3:

Таблица 3 - Исходный уровень защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределеннаяИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городскаяИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;			
локальнаяИСПДн, развернутая в пределах одного здания			
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			
ИСПДн, имеющая одноточечный выход в сеть общего пользования;			
ИСПДн, физически отделенная от сети общего пользования			
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;			
запись, удаление, сортировка;			
модификация, передача			
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			
ИСПДн с открытым доступом			
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДнИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн			
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует			

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
информация, позволяющая идентифицировать субъекта ПДн)			
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
Указать ваш тип ИСПДн			

2)Указать показатель исходной защищенности Y_1;

3)Определить вероятность реализации УБПДн для всех типов угроз ИСПДн данного класса (маловероятно, низкая вероятность, средняя и высокая вероятность).

Исходная степень защищенности определяется следующим образом:

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70 % характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70 % характеристик ИСПДн соответствуют уровню не ниже «среднего» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по п. 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

0 – для маловероятной угрозы;
2 – для низкой вероятности угрозы;
5 – для средней вероятности угрозы;
10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y1 + Y2)/20$. По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом: если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой; если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней; если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой; если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

4)Заполнить таблицу 4.

Вероятность реализации угроз безопасности персональных данных будет определяться экспертным методом в соответствии с Методикой и на основании результатов исследования ИСПДн.

Таблица 4 - Вероятность реализации угроз безопасности персональных данных

Угроза	Вероятность Y2
Угрозы утечки информации по техническим каналам	
Угрозы утечки видовой информации:	
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны	
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн	
Угрозы утечки информации по каналам ПЭМИН:	
Утечка информации по сетям электропитания ИСПДн	
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	
Утечка информации из ИСПДн за счет побочного излучения технический средств	
Преднамеренное электромагнитное воздействие на элементы ИСПДн	
Угрозы НСД к персональным данным	
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):	
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн	
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн	
Внедрение в ИСПДн вредоносных программ	
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):	
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации	
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей	
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	
Внедрение ложного объекта сети	
Сетевые атаки типа «Отказ в обслуживании»	

Угроза	Вероятность Y2
Удаленный запуск приложения в ИСПДн	
Внедрение по сети вредоносных программ	
Угрозы физического доступа к элементам ИСПДн:	
Хищение элементов ИСПДн, содержащих ПДн	
Хищение отчуждаемых носителей информации, содержащих ПДн	
Вывод из строя элементов ИСПДн	
Внедрение в ИСПДн аппаратных закладок	
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн	
Утрата паролей доступа к ИСПДн	
Искажение или уничтожение информации в результате ошибок пользователя	
Выход из строя аппаратно-программных средств ИСПДн	
Сбой системы электроснабжения ИСПДн	
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами	

5)Определить возможности реализации угроз безопасности персональных данных.

Для определения возможности реализации угроз безопасности персональных данных в соответствии с Методикой использованы следующие показатели:

- уровень исходной защищенности ИСПДн;
- вероятность реализации угроз безопасности персональных данных.

Результаты определения возможности реализации угроз привести в таблице 5.

Таблица 5 - Возможность реализации угроз безопасности персональных данных

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
Угрозы утечки информации по техническим каналам			
Угрозы утечки видовой информации:			
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	5	0,75	Высокая
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	2	0,6	Средняя

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны			
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн			
Угрозы утечки информации по каналам ПЭМИН:			
Утечка информации по сетям электропитания ИСПДн			
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны			
Утечка информации из ИСПДн за счет побочного излучения технический средств			
Преднамеренное электромагнитное воздействие на элементы ИСПДн			
Угрозы НСД к персональным данным			
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):			
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн			
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн			
Внедрение в ИСПДн вредоносных программ			

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):			
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации	10	1	Очень высокая
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей			
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа			
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных			
Внедрение ложного объекта сети			
Сетевые атаки типа «Отказ в обслуживании»			
Удаленный запуск приложения в ИСПДн			
Внедрение по сети вредоносных программ			
Угрозы физического доступа к элементам ИСПДн:			
Хищение элементов ИСПДн, содержащих ПДн			
Хищение отчуждаемых носителей информации, содержащих ПДн			
Вывод из строя элементов ИСПДн			
Внедрение в ИСПДн аппаратных закладок			
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн			
Утрата паролей доступа к ИСПДн			

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
Искажение или уничтожение информации в результате ошибок пользователя			
Выход из строя аппаратно-программных средств ИСПДн			
Сбой системы электроснабжения ИСПДн			
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами			

6)Определить актуальность угроз безопасности персональных данных.

Определение актуальных угроз безопасности персональных данных проводится экспертным методом. Результаты привести в таблице 6. (Таблица составлена для угроз определенного класса ИСПДн, ваш список угроз может отличаться).

Таблица 6 - Определение актуальных угроз нарушения безопасности персональных данных

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Угрозы утечки информации по техническим каналам			
Угрозы утечки акустической информации:			
В ИСПДн не реализованы функции голосового ввода ПДн и воспроизведения ПДн акустическими средствами			Неактуальна
Угрозы утечки видовой информации:			
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	Высокая	Средняя	Актуальная
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	Средняя	Средняя	Актуальная
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими			

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
наблюдение (регистрацию) из-за границ контролируемой зоны			
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн			
Угрозы утечки информации по каналам ПЭМИН:			
Утечка информации по сетям электропитания ИСПДн			
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны			
Утечка информации из ИСПДн за счет побочного излучения технический средств			
Преднамеренное электромагнитное воздействие на элементы ИСПДн			
Угрозы НСД к персональным данным			
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):			
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн			
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн			
Внедрение в ИСПДн вредоносных программ			
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):			

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации			
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей			
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа			
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Очень высокая	Средняя	Актуальная
Внедрение ложного объекта сети	Очень высокая	Высокая	Актуальная
Сетевые атаки типа «Отказ в обслуживании»			
Удаленный запуск приложения в ИСПДн			
Внедрение по сети вредоносных программ			
Угрозы физического доступа к элементам ИСПДн:			
Хищение элементов ИСПДн, содержащих ПДн			
Хищение отчуждаемых носителей информации, содержащих ПДн			
Вывод из строя элементов ИСПДн			
Внедрение в ИСПДн аппаратных закладок			
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн			
Утрата паролей доступа к ИСПДн			
Искажение или уничтожение информации в результате ошибок пользователя			

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Выход из строя аппаратно-программных средств ИСПДн			
Сбой системы электроснабжения ИСПДн			
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами			

7)Оценить степень возможного ущерба от реализации угрозы безопасности информации. Заполнить таблицу 7.

Таблица 7 - Оценка степени ущерба

1. Вероятность (возможность) реализации угрозы (Yj)	2. Степень возможного ущерба (Xj)		
	3. Низкая	4. Средняя	5. Высокая
6. Низкая	7.	8.	9.
10. Средняя	11.	12.	13.
14. Высокая	15.	16.	17.

Отчет

Результат выполнения работы необходимо оформить в виде отчета по лабораторной работе и защитить преподавателю. Для успешной защиты необходимо указать ответы на все пункты задания по ходу выполнения работы и уметь ответить на вопросы по теме лабораторной работы.

Лабораторная работа № 4
Выявление возможных уязвимостей и каналов несанкционированного доступа

Цель работы: Описание каналов реализации угроз информационной безопасности и основных способов реализации угроз ИБ для ИСПДн данного типа. Составление списка уязвимостей для вашего объекта, основываясь на актуальных угрозах.

При определении основных способов реализации угроз информационной безопасности ресурсов ИСПДн, необходимо учитывать необходимость обеспечения информационной безопасности на всех этапах жизненного цикла ИСПДн, компонентов, условий функционирования ИСПДн, а также - предположения о вероятных нарушителях.

Возможны следующие способы реализации угроз информационной безопасности ИСПДн:

1) несанкционированный доступ к защищаемой информации с использованием штатных средств ИСПДн ТБ и недостатков механизмов разграничения доступа;

2) негативные воздействия на программно-технические компоненты ИСПДн ТБ вследствие внедрения компьютерных вирусов и другого вредоносного программного обеспечения;

3) маскировка под администратора ИСПДн ТБ, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых ИСПДн ТБ;

4) осуществление прямого хищения (утраты) элементов ИСПДн ТБ, носителей информации и производственных отходов (распечаток, списанных носителей);

5) компрометация технологической (аутентификационной) информации путем визуального несанкционированного просмотра и подбора с использованием штатных средств, предоставляемых ИСПДн ТБ;

6) методы социальной инженерии для получения сведений об ИСПДн ТБ, способствующих созданию благоприятных условий для применения других методов;

7) использование оставленных без присмотра незаблокированных средств администрирования ИСПДн ТБ и АРМ;

8) сбои и отказы программно-технических компонентов ИСПДн ТБ;

9) внесение неисправностей, уничтожение технических и программно-технических компонентов ИСПДн ТБ путем непосредственного физического воздействия;

10) осуществление несанкционированного доступа к информации при ее передаче.

Классы уязвимостей по ГОСТ:

Уязвимости по области происхождения:

- уязвимости кода;
- уязвимости конфигурации;
- организационные уязвимости;
- многофакторные уязвимости.

Уязвимости по типу недостатков информационной системы:

- уязвимости, связанные с неправильной настройкой параметров ПО;
- уязвимости, связанные с неполнотой проверки входных данных;
- уязвимости, связанные с возможностью перехода по ссылкам;
- уязвимости, связанные с возможностью внедрения команд ОС;
- уязвимости, связанные с межсайтовым скриптингом (выполнением сценариев);
- уязвимости, связанные с внедрением произвольного кода;
- уязвимости, связанные с переполнением буфера памяти;
- уязвимости, связанные с недостатками, приводящими к утечке/раскрытию информации ограниченного доступа;
- уязвимости, связанные с управлением полномочиями (учетными данными);
- уязвимости, связанные с управлением разрешениями, привилегиями и доступом;
- уязвимости, связанные с аутентификацией;
- уязвимости, связанные с криптографическими преобразованиями;
- уязвимости, связанные с подменой межсайтовых запросов;
- уязвимости, связанные с управлением ресурсами.

Уязвимости по месту возникновения (проявления):

- уязвимости в общесистемном (общем) программном обеспечении;
- уязвимости в прикладном программном обеспечении;
- уязвимости в специальном программном обеспечении;
- уязвимости в технических средствах;
- уязвимости в портативных технических средствах;
- уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании;
- уязвимости в средствах защиты информации.

Ход работы

1. Определить возможные каналы несанкционированного доступа
2. Указать основные уязвимости, которые могут быть использованы для реализации угроз для данного списка каналов
3. Определить основные способы реализации угроз ИБ для ИСПДн

Отчет

Результат выполнения работы необходимо оформить в виде отчета по лабораторной работе и защитить преподавателю. Для успешной защиты необходимо указать ответы на все пункты задания по ходу выполнения работы и уметь ответить на вопросы по теме лабораторной работы.

Лабораторная работа № 5
Определение класса средств криптографической защиты информации. Разработка модели угроз по документам ФСБ

Перед выполнением работы необходимо ознакомиться с интернет ресурсом Информация ФСБ России :: Федеральная Служба Безопасности (fsb.ru) и документами в разделе «Нормативные правовые акты»:

- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года, № 149/7/2/6-432).

- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (утверждены приказом ФСБ России от 10 июля 2014 года № 378)

Цель работы: определить класс средств криптографической защиты информации для своего объекта. Написать модель угроз, указать обобщенные возможности источников атак и реализацию угроз безопасности информации, определяемую по возможностям источников атак.

Класс средств криптографической защиты напрямую зависит от возможностей нарушителя и устанавливается в соответствии с 378 приказом ФСБ (для персональных данных, а для других видов информации таких требований просто нет).

Ход работы

1. В соответствии с приказом № 378 определить класс средства криптографической защиты информации для своего объекта.

- СКЗИ класса КА в случаях, когда для информационной системы актуальны угрозы 1-го типа;
- СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2-го типа;
- СКЗИ класса КС1 и выше в случаях, когда для информационной системы актуальны угрозы 3-го типа.

- СКЗИ класса КС3 применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа перечисленных в пунктах 10 и 11 настоящего документа и не менее одной из следующих дополнительных возможностей:

а) **физический доступ к СВТ, на которых реализованы СКЗИ и СФ**; б) возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

- такие распространенные СКЗИ, как, например ViPNet Client или КриптоПРО CSP реализованы на рабочих станциях пользователей;
- пользователи – потенциальные нарушители;
- потенциальный нарушитель имеет физический доступ к средствам вычислительной техники, на которых реализованы их СКЗИ и среда функционирования.

Таким образом, обосновать более низкий класс СКЗИ можно только обосновав, что наши пользователи не являются потенциальными нарушителями, или использовать только криптошлюзы, которые расположены в серверных помещениях, в которые, в свою очередь, имеют доступ только привилегированные пользователи, которых мы исключили из списка потенциальных нарушителей.

2. В соответствии с приказом № 149 составить модель угроз и заполнить таблицы 8 и 9: указать обобщенные возможности источников атак и реализацию угроз безопасности информации, определяемую по возможностям источников атак.

Таблица 8 – Обобщенные возможности источников атак

N	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области	

	использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	

Таблица 9 - Актуальные угрозы

N	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	проведение атаки при нахождении в пределах контролируемой зоны		
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;		
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;		
1.4	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		
2.1	физический доступ к СВТ, на которых реализованы СКЗИ и СФ;		

2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		
3.1	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (не декларированных) возможностей прикладного ПО;		
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;		
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.		
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (не декларированных) возможностей системного ПО;		
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ;		
4.3	возможность воздействовать на любые компоненты СКЗИ и СФ.		

Отчет

Результат выполнения работы необходимо оформить в виде отчета по лабораторной работе и защитить преподавателю. Для успешной защиты необходимо указать ответы на

все пункты задания по ходу выполнения работы и уметь ответить на вопросы по теме лабораторной работы.

Лабораторная работа № 6
Оценка актуальных угроз безопасности информации

Перед выполнением работы необходимо ознакомиться с интернет ресурсом https://fstec.ru/ документом в разделе «Техническая защита информации»:

1. - "МЕТОДИЧЕСКИЙ ДОКУМЕНТ. МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ" (УТВ. ФСТЭК РОССИИ 05.02.2021)

Цель работы: Определение негативных последствий от реализации (возникновения) угроз безопасности информации, определение возможных объектов воздействия угроз безопасности информации, оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

Ход работы

1. Ознакомиться с приложением 3 настоящей методики и скопировать рекомендуемую структуру модели угроз.
2. Заполнить все пункты модели угроз в соответствии с приложениями документа:

2.1 Определить негативные последствия от реализации (возникновения) угроз безопасности информации и заполнить таблицу: виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации.

2.2 Определить возможные объекты воздействия угроз безопасности информации и заполнить таблицу: примеры определения объектов воздействия и видов воздействия на них.

2.3 Определить возможные цели реализации угроз безопасности информации нарушителями.

Указанные возможные цели реализации угроз безопасности информации подлежат конкретизации и могут дополняться другими целями в зависимости от особенностей области деятельности, в которой функционируют системы и сети. При оценке возможностей нарушителей необходимо исходить из того, что для повышения уровня своих возможностей нарушители 1-го вида могут вступать 50 в сговор с нарушителями 5, 6, 7, 8, 9, 10, 11, 12 видов. Нарушители 2-го вида могут вступать в сговор с нарушителями 10, 11, 12 видов. Нарушители 3-го вида могут вступать в

сговор с нарушителями 10, 11, 12 видов. В случае принятия таких предположений цели и уровни возможностей нарушителей подлежат объединению.

2.4 Оценить цели реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации.

2.5 Определить уровни возможностей нарушителей по реализации угроз безопасности информации.

2.6 Определить актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности.

2.7 Определить актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

Исходными данными для оценки актуальности угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов компьютерных атак, содержащихся в базах данных и иных информационных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

г) объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с настоящей Методикой;

д) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с настоящей Методикой;

е) актуальные способы реализации (возникновения) угроз безопасности информации.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным

последствиям: УБИi = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации.

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации.

3. Заполнить таблицу 10 по оценке актуальных угроз безопасности. Для этого необходимо выгрузить все угрозы из банка данных угроз с сайта ФСТЭК, выбрать актуальные угрозы и указать те категории угроз, которые не подходят для вашего объекта.
4. Сделать выводы о защищенности информационной системы, составе актуальных угроз безопасности и дать рекомендации по улучшению мер безопасности и составу средств защиты.

Отчет

Результат выполнения работы необходимо оформить в виде отчета по лабораторной работе и защитить преподавателю. Для успешной защиты необходимо указать ответы на все пункты задания по ходу выполнения работы и уметь ответить на вопросы по теме лабораторной работы.

Лабораторная работа № 7
Оценка эффективности средств защиты информации. Метод экспертных структурных вопросников

Цель работы: Изучить основные методы оценки эффективности средств защиты информации и применить на практике метод экспертных структурных вопросников

Задание: Сравнить известные методы оценки эффективности СЗИ и определить область применения каждого из методов. Заполнить структурные вопросники для своей организации (выдается преподавателем в печатном виде).

Метод получения информации об объекте с помощью специалистов-экспертов в определенной области широко используется в прогнозировании или принятии плановых решений, помогает оценить значимость показателей и проверить качество методик, применяемых для сбора данных, повысить обоснованность практик, рекомендаций и т.д. Для подготовки экспертизы формируется группа специалистов.

В ее задачи входят:

а) постановка проблемы, определение целей и задач экспертизы, ее границ, основных этапов;

б) разработка процедуры экспертизы;

в) отбор экспертов, проверка их компетентности и формирование групп экспертов;

г) проведение опроса и согласование оценок;

д) формализация полученной информации, ее обработка и анализ и интерпретация.

В состав группы входят специалисты в данной области знания, а также специалисты по экспертным методам (социологи, психологи, математики), всего может быть 5-7 человек.

Формирование целей и задач экспертного оценивания проводит менеджер ответственный за риски – должностное лицо, обладающее необходимыми полномочиями, знаниями и опытом управления рисками в определенном роде деятельности.

При формировании целей и задач экспертного оценивания должны учитываться следующие факторы:

- надежность и полнота имеющейся информации;
- форма представление конечных результатов – качественная или количественная;

- возможные области использования результатов экспертного оценивания рисков;
- сроки проведения экспертизы;
- наличие имеющихся ресурсов экспертного привлечения экспертов.

В основе экспертизы обычно лежит вопросник, с помощью которого и осуществляется сбор требуемой информации. В своем классическом варианте вопросник отсутствует при свободном интервью, аналитических экспертных оценках и т.п. Вопросник, или анкета, - это структурно организованный набор вопросов, каждый их которых логически связан с центральной задачей экспертизы.

Вопросы анкеты в зависимости от их содержания делятся на три группы:

а) данные о самом эксперте - его возрасте, стаже работы, образовании, научном звании, узкой специальности;

б) вопросы по существу исследуемой проблемы;

в) вопросы, позволяющие оценить мотивы, которых придерживался эксперт в своем анализе.

По форме вопросы могут быть открытыми, закрытыми и полузакрытыми, прямыми и косвенными. Для обеспечения поступления надежной и достоверной информации обычно сочетают все типы вопросов. При использовании оценочных шкал положительные и отрицательные стороны уравновешивают.

ЗАКЛЮЧЕНИЕ

Учебно-методическое пособие позволяет студентам освоить базовые знания и приобрести навыки по обеспечению информационной безопасности открытых систем, составлению модели угроз и уязвимостей и анализу действий нарушителя открытых систем.

Для углубления своих знаний в области проектирования открытых систем в защищенном исполнении студенты могут использовать учебные ресурсы, часть из которых представлена в списке литературы.

ЛИТЕРАТУРА

1. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В.В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие. – Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

3. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие/ Ю.А. Родичев. – Санкт-Петербург.: Питер, 2017. – 256 с.

4. Хореев, П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов/ П.Б. Хореев. - Москва: Academia, 2008.- 256 с.

5. Черемушкин, А. В. Информационная безопасность. Глоссарий / Под ред. С. Пазизина. – Москва: «АВАНГАРД ЦЕНТР», 2013. – 322 стр.

6. Методика оценки актуальных угроз безопасности, методический документ, Утвержден ФСТЭК России 5 февраля 2021 г.

Локальный электронный методический материал

Алина Андреевна Бабаева

ПРОЕКТИРОВАНИЕ ОТКРЫТЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Редактор Г. А. Смирнова

Уч.-изд. л. 1,7. Печ. л. 2,4

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