Предисловие

При подготовке данного учебно-методического пособия были поставлены следующие задачи:

1) описать процесс, основные концепции и технологии предотвращения утечки конфиденциальной информации;

2) рассмотреть архитектуру, особенности применения и аналитические возможности соответствующих программных решений.

Исходя из поставленных задач, была определена структура учебно-методического пособия «Основы аналитики в DLP-системах. Программный комплекс «КИБ СёрчИнформ», которое состоит из введения, восьми глав теоретической части и четырех глав лабораторного практикума, заключения и списка литературы.

Во введении обоснована актуальность темы учебно-методического пособия. В первой главе приводятся общие сведения о DLP-системах и определяется их место среди других средств защиты информации. Во второй главе анализируются решения российской компании «СёрчИнформ», входящие в программный комплекс «КИБ СёрчИнформ». Третья глава посвящена различным видам поиска информации, находящейся в корпоративной сети организации, в частности фразовому поиску, поиску по словарю, поиску похожих, поиску по атрибутам, регулярным выражениям, цифровым отпечаткам, формам и т. п. Четвертая глава знакомит обучающихся с AnalyticConsole, используемой для ручного и автоматического анализа информации. В пятой главе рассмотрен AlertCenter, осуществляющий автоматический мониторинг информационных потоков. Вопросы блокировки информации в «КИБ СёрчИнформ» детализируются в шестой главе. Аудит операций в файловой системе и прав доступа к файлам посредством «FileAuditor СёрчИнформ» описан в главе 7. В восьмой, заключительной теоретической главе изучается «Профайл

центр», предназначенный для оценки рисков, связанных с человеческим фактором.

В части, отведенной под описание лабораторного практикума, представлены четыре лабораторные работы со следующими названиями:

- «Основные компоненты программного комплекса «СёрчИнформ КИБ» и разграничение прав доступа»;
- «Основные принципы и приемы использования DLP-системы для мониторинга утечек конфиденциальной информации (на примере программного комплекса «СёрчИнформ КИБ»)»;
- «Осуществление контроля переписки и действий пользователей при помощи различных видов поиска (на примере программного комплекса «СёрчИнформ КИБ»)»;
- «Проведение расследований с использованием возможностей программного комплекса "СёрчИнформ КИБ"».

В заключении обобщаются функциональные возможности изученного средства защиты информации — DLP-системы.

Тематика учебно-методического пособия согласуется с положениями профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 533н), определяющего обобщенные трудовые функции (ОТФ), трудовые функции (ТФ), трудовые действия, необходимые умения и знания соответствующих специалистов.

Согласно этому профстандарту, освоение материалов данного учебно-методического пособия подготовит обучающихся к выполнению ОТФ «Администрирование средств защиты информации (СЗИ) в компьютерных системах и сетях (КСиС)» и ТФ «Администрирование программно-аппаратных СЗИ (ПА СЗИ) в компьютерных сетях (КС)»:

После изучения учебно-методического пособия обучающиеся будут готовы выполнять следующие трудовые действия, связанные с DLP-системами как СЗИ:

- разработка порядка применения ПА СЗИ в КС;
- формирование шаблонов конфигурации ПА СЗИ в КС;
- управление функционированием ПА СЗИ в КС;
- контроль корректности функционирования ПА СЗИ в КС.

Необходимые для этого умения:

- оценка угроз безопасности информации в КС;
- настройка правил фильтрации пакетов в КС;

- обоснование выбора используемых ПА СЗИ в КС;
- конфигурирование и контроль корректности настройки ПА СЗИ в КС;
- выбор режимов работы ПА СЗИ в КС;
- мониторинг функционирования ПА СЗИ в КА;
- анализ эффективности ПА СЗИ в КС;
- оценка оптимальности выбора ПА их режимов функционирования в КС.

Необходимые для этого знания:

- принципы построения КС;
- стек сетевых протоколов операционных систем;
- принципы функционирования сетевых протоколов, включающих криптографические алгоритмы;
- виды политик управления доступом и информационными потоками в КС;
- источники угроз ИБ в КС и меры по их предотвращению;
- состав типовых конфигураций ПА СЗИ и режимов их функционирования в КС;
- методы измерений, контроля и технических расчетов характеристик ПА СЗИ;
- принципы работы и правила эксплуатации применяемых ПА СЗИ;
- программно-аппаратные средства и методы защиты информации в КС;
- нормативные правовые акты в области защиты информации;
- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры;
- организационные меры по защите информации.

Материалы, вошедшие в учебно-методическое пособие, обеспечивают учебно-методической базой любую учебную дисциплину, относящуюся к защите конфиденциальной информации в корпоративной сети организации. Однако в полной мере данное пособие может быть востребовано при подготовке профессионалов в области управления ИБ в целом и сетевой безопасностью в частности. Поэтому оно может быть рекомендовано студентам образовательных организаций высшего образования, обучающихся по направлению подготовки 10.04.01 «Информационная безопасность» укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Кроме этого, учебно-методическое пособие может быть полезным при реализации программ дополнительного образования (курсы повышения квалификации или переподготовки кадров).

Важно подчеркнуть, что для приступающих к ознакомлению с учебно-методическим пособием есть определенные требования по предварительной подготовке. Например, следует знать основы теории ИБ и комплексный подход к обеспечению ИБ (ОИБ), уязвимости и угрозы ИБ в информационной среде.

Авторы признательны коллегам по НИЯУ МИФИ, а также всем рецензентам.

Авторы, естественно, не претендуют на исчерпывающее изложение всех названных в работе аспектов проблем предотвращения утечки конфиденциальной информации организации, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебно-методическим пособием.