МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Новоуральский технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(НТИ НИЯУ МИФИ)
Колледж НТИ
Цикловая методическая комиссия информационных технологий

ОТЧЁТ
ПО ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЕ НА ТЕМУ

«Сравнительный анализ понятийных аппаратов различных источников в области защиты информации»

МДК 05.01 ПМ.05 «Защита информации в КС»

Специальность СПО 09.02.03
«Программирование в компьютерных системах»

очная форма обучения
на базе основного общего образования

Выполнил
студент группы КПР–47 Д
Егорушкин И.А. _____30.09.2020_____ _____
дата подпись

Проверил
преподаватель _____ _____
Горницкая И.И. дата подпись

Новоуральск 2020

Цель работы: Исследование терминологической базы, закрепление знаний основного понятийного аппарата, применяемого в области защиты информации, а также формирование навыка работы с руководящими документами по исследуемому вопросу.
Оборудование: Процессор Intel® core™ i3-2120 CPU @ 3.30GHz. 3.30GHZ, ОЗУ 2ГБ, тип системы: 32-разрядная операционная система.

Программное обеспечение: Microsoft word 2010

Документы:

[1]. Защита информации. Департамент Смоленской области по информационным технологиям. Руководящий документ ГОСТ Р 50922-2006

[2]. «Об информации, информационных технологиях и о защите информации». Защита информации. Руководящий документ от 27.07.2006 N 149-ФЗ

[3]. ГОСТ Р 50922-96 – ФСТЭК РОССИИ. Руководящий документ [ГОСТ Р 51583-2014, статья 3.3]

[4]. Автоматизированные системы в защищенном исполнении с применением системы защиты информации в соответствии с законодательством РФ. Руководящий документ ГОСТ Р 51583-2014

[5]. Понятие безопасности компьютерной информации. Объекты и элементы защиты данных в компьютерных системах. Руководящий документ ГОСТ Р ИСО/МЭК 17799—2005

[6]. Информационная безопасность. Руководящий документ ГОСТ Р ИСО/МЭК 17799—2005 [7]. Информационная безопасность. Защита информации. Способы защиты информации. Руководящий документ

[8]. Приказ об утверждении ФСТЭК РФ от 05.02.2010 N58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Руководящий документ 2008, N 12, ст. 1110; N 43, ст. 4919.

[9] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения

[10]. Основные защитные механизмы, используемые в СЗИ. Основные механизмы защиты компьютерных систем. Руководящий документ

[11]. Системы защиты от несанкционированного доступа. Руководящий документ

[12]. Средства защиты информации от несанкционированного доступа Руководящий документ ФСТЭК России № 2720 от 25.09.2012

[13]. Фактор, воздействующий на защищаемую информацию Руководящий документ из п. 2.1(3) ГОСТ Р 51275-99

[14]. Факторы, воздействующие на защищаемую информацию. Руководящий документ ГОСТ Р 51275-2006 (взамен ГОСТ Р 51275-99)

[15]. Администратор безопасности. Руководящий документ

[16]. Методы менеджмента безопасности. Информационных технологий. Руководящий документ ISO/IEC TR 13335-3:1998

[17]. Методы менеджмента безопасности. Информационных технологий. Руководящий документ ГОСТ Р ИСО/МЭК ТО 13335-3—2007

[18]. Методы менеджмента безопасности. Информационных технологий. Руководящий документ ГОСТ Р ИСО/МЭК ТО 13335-3—2007

[19]. Методы менеджмента безопасности. Информационных технологий. Руководящий документ ГОСТ Р ИСО/МЭК ТО 13335-3—2007

п.п.	Термин (понятие)	Определение	ИСТОЧНИК (ГОСТ, ОСТ, РД, учебник, пособие, статья, др. источники)
1.	Защита информации	Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.	[1]
		Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации.	[2]
2.	Система защиты информации автоматизированной системы	Совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.	[3]

		Система защиты информации АС должна обеспечивать комплексное решение задач по защите информации от следующих угроз: — несанкционированный доступ (НСД) к информации АС; — утечка защищаемой информации по техническим каналам; — несанкционированные воздействия на информацию (на носители информации);	[4]
3.	Безопасность компьютерной информации	Под информационной безопасностью РФ понимается состояние защищённости её национальных интересов и информационной сфере, определяющей совокупность интересов личности, общества и государства. В частности, среди основных задач, кои необходимо решить в области безопасности является обеспечение эффективного функционирования электронного бизнеса	[5]
		Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные.	[6]

4.	Метод защиты	На практике используют несколько групп методов защиты, в том числе: препятствие на пути предполагаемого похитителя, которое создают физическими и программными средствами; управление, или оказание воздействия на элементы защищаемой системы; маскировка, или преобразование данных, обычно – криптографическими способами; регламентация, или разработка нормативно- правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению; принуждение, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными; побуждение, или создание условий, которые мотивируют пользователей к должному поведению.	[7]

		Методами и способами защиты информации от несанкционированного доступа являются: - реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам; - ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации; - разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации; - регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;	[8]

5.	Механизм защиты	В NetWare реализованы три уровня защиты данных Здесь под аутентификацией понимается: - процесс подтверждения подлинности клиента при его подключении к сети, - процесс установления подлинности пакетов, передаваемых между сервером и рабочей станцией. Права по отношению к файлу (каталогу) определяют, какие операции пользователь может выполнить с файлом (каталогом). Администратор может для каждого клиента сети определить права по отношению к любому сетевому файлу или каталогу.	[9]
		Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и НСД к информации используются следующие основные методы зашиты: - идентификация (именование и опознавание), аутентификация (подтверждение подлинности) пользователей системы; - разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям; - регистрация и	

		оперативное оповещение о событиях, происходящих в системе; (аудит)	[10]

		- криптографическое закрытие хранимых и передаваемых по каналам связи данных; - контроль целостности и аутентичности (подлинности и авторства) данных; - выявление и нейтрализация действий компьютерных вирусов; - затирание остаточной информации на носителях; - выявление уязвимостей (слабых мест) системы; - изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы и т.д.); - обнаружение атак и оперативное реагирование. - Резервное копирование - Маскировка.	
6.	Защита от несанкционированного доступа	Это программные и/или аппаратные средства, позволяющие предотвратить попытки несанкционированного доступа, такие как неавторизованный физический доступ, доступ к файлам, хранящимся на компьютере, уничтожение конфиденциальных данных.	[11]

		Средства защиты от несанкционированного доступа (СЗИ от НСД) - программные, технические или программно- технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации.	
		СЗИ от НСД может выполнять функции - идентификация и аутентификация пользователей и устройств; - регистрация запуска программ и процессов; - реализация необходимых методов, типов и правил разграничения доступа; - управление информационными потоками между устройствами; - учет носителей информации и другие функции.	[12]
7.	Фактор, воздействующий на защищаемую информацию	Явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.	[13]

		Под факторами, воздействующими на защищаемую информацию, подразумевают явления, действия или процессы, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации или блокирование доступа к ней. Различают объективные и субъективные факторы и в каждом классе выделяют внешние и внутренние факторы. Подробный перечень факторов можно найти в ГОСТ Р 51275- 2006 (взамен ГОСТ Р 51275-99) , который распространяется на требования по организации ЗИ при создании и эксплуатации объектов информатизации, используемых в различных	

		областях деятельности (обороны, экономики, науки и других областях). Значение некоторых используемых терминов: побочное электромагнитное излучение – излучение, возникающее при работе технических средств обработки информации; паразитное электромагнитное излучение – излучение, вызванное паразитной генерацией в электрических цепях технических средств обработки информации; «маскарад» – маскировка под зарегистрированного пользователя.	[14]
8.	Администратор защиты	Администратор безопасности является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники, в пределах своей зоны ответственности. Изменение зоны ответственности администратора безопасности производится приказом руководителя СИБ в случае изменения организационной структуры или по предложению СИБ.	[15]

9.	Способы управления безопасностью информационных технологий	Процесс управления безопасностью информационных технологий основывается на принципах, изложенных в ИСО/МЭК 13335- 1, и может быть реализован как в масштабе всей организации, так и в конкретной ее части. На схеме 1) приведены основные этапы этого процесса, а также показана обратная связь между результатами процесса и его отдельными частями. Такая обратная связь должна устанавливается по мере необходимости как в пределах продолжительности одного из этапов, так и после завершения одного или нескольких этапов. Данная схема демонстрирует основные направления, рассматриваемые в настоящем стандарте.	[16]
10.	Цели и стратегия безопасности информационных технологий	В качестве первого шага в процессе управления безопасностью информационных технологий необходимо рассмотреть вопрос о том, какой общий уровень риска является приемлемым для данной организации. Правильно выбранный уровень приемлемого риска и, соответственно, допустимый уровень безопасности являются ключевыми моментами успешного управления безопасностью.	[17]

11.	Политика безопасности информационных технологий	Политика безопасности информационных технологий должна вырабатываться на основе содержания стратегии и целей создания системы обеспечения безопасности. Важно сформировать политику безопасности и затем проводить ее в соответствии с направленностью деятельности организации, состоянием обеспечения безопасности, содержанием политики в области информационных технологий, а также с учетом положений законодательства и нормативных документов в области обеспечения безопасности.	[18]
12.	Основные варианты стратегии анализа риска организации	Прежде чем приступить к любым действиям, связанным с анализом риска, организация должна иметь стратегию проведения такого анализа, причем составные части этой стратегии (методы, способы и т.д.) должны быть отражены в содержании политики обеспечения безопасности информационных технологий. Эти методы и критерии выбора вариантов стратегии анализа риска должны отвечать потребностям организации. Стратегия анализа риска должна обеспечивать соответствие выбранного варианта стратегии условиям осуществления деловых операций и приложения усилий по обеспечению безопасности в тех областях, где это действительно необходимо.	[19]

Вывод: В ходе работы было изучено терминологической базы, закрепление знаний основного понятийного аппарата, применяемого в области защиты информации, а также формирование навыка работы с руководящими документами по исследуемому вопросу