Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО»

Факультет экономический
Кафедра информационных технологий

СОГЛАСОВАНО
Заведующий кафедрой
_____О.Б.Хорошко
29. 05 2026 г.

СОГЛАСОВАНО
Декан факультета
_____А.В.Ковтунов
07. 07 2026 г.

ЭЛЕКТРОННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности 6-05-0611-01 Информационные системы и технологии

Составитель: Пархимович А.В., старший преподаватель кафедры информационных технологий учреждения образования Федерации профсоюзов Беларуси «Международный университет МИТСО»

Рассмотрено и рекомендовано к утверждению на заседании кафедры информационных технологий
29. 05 2026 г., протокол № 11

Утверждено на заседании научно-методического совета учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
07. 07. 2026 г., протокол № 6

РЕЦЕНЗЕНТЫ:
Кафедра микропроцессорных систем и сетей УО «Белорусский государственный университет информатики и радиоэлектроники» (Кашникова И.В., заведующий кафедрой);
Волк В.В., начальник отдела информационных технологий УО ФПБ «Международный университет «МИТСО»

Регистрационный № УД-086-26/р

Регистрационное свидетельство № 1202544653 от 03.11.2025

новый, как актуализация „Информационная безопасность" 20.07.2026

Актуализирован
заседание кафедры _____
_____ учреждения
образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
_____20____, протокол №

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4
УЧЕБНАЯ ПРОГРАММА 6
I. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ 21
Предмет, содержание и задачи курса, его место в системе подготовки специалиста. Формы отчетности 21
Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе 25
Информационная безопасность личности, общества и государства: социально-правовые аспекты 29
Компьютерная система как объект защиты информации. Угрозы информационной безопасности в компьютерных системах 39
Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации 42
Повышение эксплуатационной надежности компьютерных систем 46
Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации 49
Комплексная защита информации в компьютерных системах (КСЗИ). Концепция КСЗИ в компьютерных системах. функционирования КСЗИ 53
II. ПРАКТИЧЕСКИЙ РАЗДЕЛ 57
Планы и задания для практических занятий 57
III. РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ 67
Темы рефератов 67
Примерный перечень вопросов к зачету 68
IV. ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ 70
Перечень рекомендуемой литературы 70
Нормативные правовые акты 71

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Электронный учебно-методический комплекс (ЭУМК) подготовлен в соответствии с учебной программой Учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО» по дисциплине «Основы информационной безопасности» для специальности 6-05-0611-01 «Информационные системы и технологии».

Цель ЭУМК – обеспечение максимальной доступности и системности изучаемого материала по дисциплине, формирование у студентов специализированных компетенций в области защиты информации. Практическая значимость состоит в том, что данный ЭУМК позволяет структурировать учебную деятельность студентов, освоить методы анализа рисков и подходы к управлению инцидентами в сфере информационной безопасности.

Основными структурными элементами ЭУМК являются:

• Учебная программа по дисциплине, составленная на основе образовательного стандарта ОСВО 6-05-0611-01-2023.

• Теоретический раздел, включающий конспект лекций для теоретического изучения. Содержание разделов охватывает основы информационной безопасности, угрозы и методы защиты в компьютерных системах, а также организационное и комплексное обеспечение информационной безопасности (КСЗИ).

• Практический раздел, содержащий учебно-методические материалы для проведения практических занятий. Темы работ включают анализ уязвимостей компьютерных систем, разработку политик информационной безопасности, сравнительный анализ средств защиты информации и проектирование концепции комплексной системы защиты информации (КСЗИ).

• Раздел контроля знаний, примерный перечень вопросов к зачету, а также темы рефератов.

• Вспомогательный раздел, в котором приведены рекомендации по освоению дисциплины, перечень основной и дополнительной литературы, а также нормативных правовых актов Республики Беларусь в области информационной безопасности.

Рекомендации по организации работы с ЭУМК.

Для лучшего усвоения материала студентам рекомендуется сначала ознакомиться с учебной программой по дисциплине «Основы информационной безопасности». Усвоение материала по каждой из тем рекомендуется начинать с изучения соответствующей лекции («Теоретический раздел»), после чего следует ответить на вопросы для самоконтроля и выполнить задания практических занятий («Практический раздел»). Проверка знаний проводится путем решения практических задач, защиты докладов и ответов на вопросы из перечня для

промежуточной аттестации («Раздел контроля знаний»). Студентам рекомендуется использовать материалы ЭУМК для осуществления активной самостоятельной работы при изучении дисциплины, подготовки к аудиторным занятиям и сдаче зачета.

Учреждение образования Федерации профсоюзов Беларуси
«Международный университет МИТСО»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
Федерации профсоюзов Беларуси
«Международный университет «МИТСО»
_____М.А.Юрочкин
_____ 2024 г.
Регистрационный № УД-067/02-24/уч.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности

6-05-0611-01 Информационные системы и технологии

2024 г.

Контрольный экземпляр

Учебная программа учреждения высшего образования составлена на основе Образовательного стандарта высшего образования ОСВО 6-05-0611-01-2023 (общее высшее образование), для специальности 6-05-0611-01 Информационные системы и технологии, утвержденного Постановлением Министерства образования Республики Беларусь 10.08.2023 г. № 246 и учебного плана учреждения образования федерации профсоюзов Беларуси «Международный университет «МИТСО» для специальности 6-05-0611-01 «Информационные системы и технологии», утвержденного 01.03.2023 рег. № 6-05-0611-01/уч.

СОСТАВИТЕЛЬ:
Балашов О.С., преподаватель кафедры информационных технологий учреждения образования Федерации профсоюзов Беларуси "Международный университет "МИТСО"

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой информационных технологий учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
(протокол № 4 от 28.11.2024);

Научно-методическим советом учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
(протокол № 3 от 20.12.2024)

СОГЛАСОВАНО
Декан экономического факультета _____А.В.Ковтунов

Заведующий библиотекой _____О.О.Бабарикина

Нормоконтроль
ведущий специалист УМУ
_____Г.Д.Лагунович

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дисциплина «Основы информационной безопасности» входит составной частью в систему дисциплин, обеспечивающих подготовку специалистов по специальности 6-05-0611-01 «Информационные системы и технологии», относится к циклу дисциплин модуля «Общеинженерная подготовка» и изучается в тесной взаимосвязи с учебными дисциплинами: «Физика», «Теория вероятностей и математическая статистика», «Технологии разработки программного обеспечения» «Метрология, стандартизация и сертификация (в информационных технологиях)».

Целью курса является овладение знаниями и навыками для решения прикладных задач по обеспечению защиты информации в информационных технологиях, а также объектах различных категорий.

Задачами изучения дисциплины являются:

овладение студентами понятийным аппаратом в области информационной безопасности и защиты информации;

установление и раскрытие структуры угроз защищаемой информации;

изучение базовых содержательных положений в области информационной безопасности и защиты информации;

раскрытие различных форм представления информации в проблемах обеспечения информационной безопасности.

Освоение учебной дисциплины «Основы информационной безопасности» должно обеспечить у обучающихся формирование **специализированных компетенций**: обеспечивать безопасность информации с учетом способов ее представления и модели нарушителя.

В результате изучения учебной дисциплины студент должен

знать: нормативно-правовое, организационно-техническое и техническое обеспечение технологий информационной безопасности;

уметь: проектировать и проводить оценку эффективности систем защиты информации в информационных технологиях, а также объектах различных категорий;

иметь навыки: владения методами анализа рисков, подходами к управлению инцидентами в области информационной безопасности.

Распределение аудиторных часов по видам занятий и семестрам.
Виды и формы аттестации

Семестр	Количество академических часов							Самост. работа	Форма промежуточной аттестации
	Всего	Аудит.	Из них						
			Лекции	Лабор. занятия	Практ. занятия	Семинары	УСР[1]		
Очная (дневная) форма получения высшего образования									
4	108	48	28		10		10	60	Зач.
Всего	108	48	28		10		10	60	

[1] Управляемая самостоятельная работа

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Раздел 1. Основы информационной безопасности

Тема 1.1. Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности

Определение информационной безопасности и ее цели. Предмет и структура курса: Основные разделы и темы. Задачи курса: знания, умения и навыки, которые должны быть приобретены. Место курса в системе других дисциплин учебного плана.

Тема 1.2. Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе

Понятие постиндустриального общества и его основные характеристики. Роль информации как ключевого ресурса в современном обществе. Информатизация общества: положительные и отрицательные последствия.

Тема 1.3. Информационная безопасность личности, общества и государство: социально-правовые аспекты.

Информационная безопасность личности: право на неприкосновенность частной жизни, защита персональных данных. Информационная безопасность общества: защита от дезинформации, пропаганды, экстремизма. Информационная безопасность государства: защита государственной тайны, обороноспособности, критической инфраструктуры.

Раздел 2. Угрозы и методы защиты информации в компьютерных системах

Тема 2.1. Компьютерная система как объект защиты информации. Угрозы информационной безопасности в компьютерных системах

Определение компьютерной системы и ее основные компоненты: аппаратное обеспечение, программное обеспечение, данные, персонал. Классификация компьютерных систем по различным признакам: размер, назначение, степень защищенности. Компьютерные системы как объект защиты информации: ценность информации, уязвимости, риски.

Тема 2.2. Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации

История развития концепции информационной безопасности в компьютерных системах: от защиты от физического доступа до комплексной защиты от киберугроз. Основные этапы развития средств и методов защиты

информации. Классификация средств защиты информации: аппаратные, программные, организационные.

Тема 2.3. Повышение эксплуатационной надежности компьютерных систем

Понятие эксплуатационной надежности компьютерных систем и ее основные показатели. Факторы, влияющие на эксплуатационную надежность компьютерных систем: качество аппаратного и программного обеспечения, условия эксплуатации, квалификация персонала.

Раздел 3. Организационное и комплексное обеспечение информационной безопасности

Тема 3.1. Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации

Роль организационного обеспечения в системе защиты информации. Основные принципы организационного обеспечения защиты информации. Организационная структура системы защиты информации: распределение ответственности, полномочий и ресурсов.

Тема 3.2. Комплексная защита информации в компьютерных системах (КСЗИ). Концепция КСЗИ в компьютерных системах. Функционирования КСЗИ

Понятие комплексной системы защиты информации (КСЗИ) и ее цели. Принципы построения КСЗИ: эшелонированность, непрерывность, адекватность, экономическая целесообразность. Этапы создания КСЗИ: анализ рисков, разработка концепции, проектирование, внедрение, эксплуатация, совершенствование.

III. УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения высшего образования

Номер раздела, темы	Название раздела, темы	Всего часов	Количество аудиторных часов					Самостоят. работа	Литерату-ра	Форма контроля
			Лекции	Практич. занятия	Семинар. занятия	Лаборатор. занятия	Кол-во часов УСР			
4 семестр										
1.	**Основы информационной безопасности**	**36**	**8**	**2**			**4**	**22**		
1.1.	Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности	12	2				2	8	[1], [3], [18], [20]	УО, РПЗ
1.2	Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе	8	2					6	[1], [2], [4], [15]	
1.3.	Информационная безопасность личности, общества и государство: социально-правовые аспекты.	16	4	2			2	8	[5], [8], [17]	УО, РПЗ, Р,УД
2.	**Угрозы и методы защиты информации в компьютерных системах**	**42**	**12**	**4**			**4**	**22**		
2.1.	Компьютерная система как объект защиты информации. Угрозы информационной безопасности в компьютерных системах	16	4	2			2	8	[4], [6], [10]	УО, УД
2.2.	Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации	16	4	2			2	8	[7], [9], [11], [19]	УО, РПЗ
2.3.	Повышение эксплуатационной надежности компьютерных систем	10	4					6	[7], [9], [21], [22]	Р(ТА)[2]
3.	**Организационное и комплексное обеспечение информационной безопасности**	**30**	**8**	**4**			**2**	**16**		
3.1.	Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации	14	2	2			2	8	[12], [3], [23]	УО, УД
3.2.	Комплексная защита информации в компьютерных системах (КСЗИ). Концепция КСЗИ в компьютерных системах. Функционирования КСЗИ	16	6	2				8	[13], [14], [16]	УО, РПЗ
	Всего	**108**	**28**	**10**			**10**	**60**		**Зач.**

[2] Текущая аттестация

IV. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Якимахо, А. П. Управление интеллектуальной собственностью в Республике Беларусь / А. П. Якимахо, Г. Е. Ясников, И. А. Рудаков; под ред. Г. Е. Ясникова. – Минск : Дикта, 2011.

2. Якимахо, А. П. Управление объектами интеллектуальной собственности в Республике Беларусь / А. П. Якимахо. – Минск : Амалфея, 2005. – 472 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

3. Гвоздек, М. Справочник по технике для видеонаблюдения. Планирование, проектирование, монтаж / М. Гвоздек. – М. : Техносфера, 2010. – 543 с.

4. Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В.А. Тихонов. – М. : Горячая линия-Телеком, 2011. – 272 с.

5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – М. : Издат. дом «Форум» : Инфра-М, 2011. – 416 с.

6. Деднев, М. А. Защита информации в банковском деле и электронном бизнесе / М. А. Деднев, Д. В. Дыльнов, М. А. Иванов. – М. : Кудиц-образ, 2004. – 512 с.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

7. Концепция национальной безопасности Республики Беларусь, утв. решением Всебелорусского народного собрания от 25 апреля 2024 года № 5 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. - Минск, 2024.

8. О некоторых вопросах развития информационного общества в Республике Беларусь : Указ Президента Респ. Беларусь от 08 нояб. 2011 г. № 515 : в ред. от 22 июня 2023 г. № 178 // ЭТАЛОН : информ.-поисковая система (дата обращения: 11.03.2025).

9. О Концепции информационной безопасности Республики Беларусь: постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1 // ЭТАЛОН: информ.-поисковая система (дата обращения 12.03.2025).

10. Об информации, информатизации и защите информации: Закон Респ. Беларусь от 10 нояб. 2008г. №455-З: в ред. от 10.10.2022№209-З//ЭТАЛОН: информ.-поисковая система (дата обращения 12.03.2025).

11. Охрана объектов и физических лиц. Термины и определения : СТБ 1250-2000. – Введ. 01.04.2001. – Минск : БелГИСС, 2000. – 20 с.

12. Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных

системах: СТБ 34.101.70-2016. – Введ. 01.04.2017. – Минск : НИИ ТЗИ, 2016. – 40 с.

13. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: СТБ ISO/IEC 27001-2016. – Введ. 01.10.2016 (с отменой на территории СТБ ISO/IEC 27001-2011). – Минск : БелГИСС, 2016. – 28 с.

14. Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности: СТБ ISO/IEC 27003-2014. – Введ. 01.02.2015. – Минск : НИИ ТЗИ, 2014. – 68 с.

15. Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности: СТБ КОЯЕС 27005-2012. – Введ. 01.01.2013. – Минск : БелГИСС, 2012. – 68 с.

16. Охрана объектов. Требования по применению технических средств и систем охраны: ТКИ № 627-2018 (33030). – Введ. 01.01.2019 (с отменой на территории РБ РД 28/3.006-2005). – Минск : ДО МВД РБ, 2018. – 18 с.

17. Охрана объектов. Охрана объектов. Обеспечение технической укрепленности объектов: ТКП 652-2020 (33030). – Введ. 01.01.2021 (с отменой на территории РБ РД 28/3.012-2005). – Минск: Стройтехнорм, 2020. – 55 с.

СРЕДСТВА ОБУЧЕНИЯ

1. Система дистанционного обучения "Moodle".
2. Оборудованный интернет-доступом компьютерный класс с установленным специальным программным обеспечением.
3. Мультимедийная аппаратура, электронные учебнонаглядные пособия (презентации, методические материалы).

СРЕДСТВА ДИАГНОСТИКИ РЕЗУЛЬТАТОВ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Диагностика результатов образовательной деятельности обучающихся осуществляется в ходе проведения всех видов занятий, самостоятельной работы и текущей аттестации по учебной дисциплине.

Текущая аттестация обучающихся проводится в течение семестра в целях периодического контроля и оценки результатов их учебной деятельности по учебной дисциплине с выставлением отметок.

Текущий контроль проводится строго в соответствии с учебно-методической картой дисциплины.

Обучающийся должен в обязательном порядке участвовать во всех контрольных мероприятиях текущего контроля, предусмотренных учебной программой дисциплины.

Основными **формами контроля** знаний по учебной дисциплине являются:

устный опрос	УО;
устный доклад	УД;

реферат Р;
решение практических задач РПЗ.

Форма текущей аттестации по учебной дисциплине:
реферат Р.

К промежуточной аттестации по учебной дисциплине, модулю обучающиеся допускаются при условии успешного прохождения текущей аттестации, предусмотренной учебной программой в текущем семестре.

Формой промежуточной аттестации является:
зачет зач.

ПЕРЕЧЕНЬ ТЕМ И ВОПРОСОВ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Целью практических занятий является углубление знаний, их систематизация и обобщение на основе изучения разнообразных источников, развития широкого спектра аналитических умений, в том числе конспектирования, рецензирования, подготовки развернутых тематических выступлений, критического сопоставления источников и т. д.

Тема 1.3. Информационная безопасность личности, общества и государство: социально-правовые аспекты

Практическое занятие 1. Разработка памятки для граждан по защите персональных данных в интернете

Основные вопросы:

1. Определение основных угроз для персональных данных в интернете и способов их защиты.
2. Формулирование простых и понятных рекомендаций для граждан по безопасному использованию интернета и защиты личной информации.

Оборудование:

оборудованный интернет-доступом компьютерный класс с установленным специальным программным обеспечением;

мультимедийная аппаратура, электронные учебнонаглядные пособия (презентации, методические материалы).

Тема 2.1. Компьютерная система как объект защиты информации. Угрозы информационной безопасности в компьютерных системах

Практическое занятие 2. Анализ уязвимостей компьютерной системы с использованием сканера безопасности

Основные вопросы:

1. Сканирование компьютерной системы на наличие известных уязвимостей с помощью специального программного обеспечения.
2. Оценка рисков, связанных с выявленными уязвимостями, и разработка рекомендаций по их устранению.

Оборудование:

оборудованный интернет-доступом компьютерный класс с установленным специальным программным обеспечением;

мультимедийная аппаратура, электронные учебнонаглядные пособия (презентации, методические материалы).

Тема 2.2. Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации

Практическое занятие 3. Сравнительный анализ средств защиты информации различных поколений

Основные вопросы:

1. Изучение эволюции средств защиты информации (от паролей до систем обнаружения вторжений) и определение их преимуществ и недостатков.

2. Сравнение эффективности различных средств защиты информации для противодействия современным угрозам.

Оборудование:

оборудованный интернет-доступом компьютерный класс с установленным специальным программным обеспечением;

мультимедийная аппаратура, электронные учебнонаглядные пособия (презентации, методические материалы).

Тема 3.1. Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации

Практическое занятие 4. Разработка политики информационной безопасности для организации

Основные вопросы:

1. Определение целей и задач политики информационной безопасности.

2. Разработка основных положений политики, касающихся управления доступом, защиты данных, реагирования на инциденты.

Оборудование:

оборудованный интернет-доступом компьютерный класс с установленным специальным программным обеспечением;

мультимедийная аппаратура, электронные учебнонаглядные пособия (презентации, методические материалы).

Тема 3.2. Комплексная защита информации в компьютерных системах (КСЗИ). Концепция КСЗИ в компьютерных системах. Функционирования КСЗИ

Практическое занятие 5. Разработка концепции создания КСЗИ для организации

Основные вопросы:

1. Определение границ КСЗИ и основных компонентов системы защиты.

2. Разработка плана внедрения КСЗИ и определение необходимых ресурсов.

Оборудование:

оборудованный интернет-доступом компьютерный класс с установленным специальным программным обеспечением;

мультимедийная аппаратура, электронные учебнонаглядные пособия (презентации, методические материалы).

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ЗАДАНИЙ И КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ УСР

№ темы, (раздела)	Тема УСР	Кол-во часов	Метод. обеспечение	Форма контро-ля
2 курс, 4 семестр (10 часов)				
1.1.	Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности	2	Интернет-ресурсы, мультимедийная аппаратура	УО, Р
1.3.	Информационная безопасность личности, общества и государство: социально-правовые аспекты	2	Интернет-ресурсы, мультимедийная аппаратура	УО, Р
2.1.	Компьютерная система как объект защиты информации. Угрозы информационной безопасности в компьютерных системах	2	Интернет-ресурсы, мультимедийная аппаратура	УО, Р
2.2.	Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации	2	Интернет-ресурсы, мультимедийная аппаратура	УО, Р
3.1.	Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации	2	Интернет-ресурсы, мультимедийная аппаратура	УО, Р

ТЕМЫ РЕФЕРАТОВ К УСР

1. Роль и место защиты информации в сфере информационных технологий.
2. Информация. Основные понятия и определения. Формы представления.
3. Классификация угроз информационной безопасности.
4. Охраняемые сведения и демаскирующие признаки.
5. Классификация технических каналов утечки информации.
6. Прямой акустический канал утечки информации.
7. Виброакустический канал утечки информации.
8. Акустоэлектрический канал утечки информации.
9. Акустооптический канал утечки информации.
10. Параметрический (акустический) канал утечки информации.
11. Электрический канал утечки информации.
12. Индукционный канал утечки информации.
13. Параметрический (электромагнитный) канал утечки информации.
14. Визуально-оптический и материально-вещественный каналы утечки информации.
15. Утечки информации по цепям заземления.
16. Утечки информации по цепям электропитания.
17. Перехват информации в телефонных каналах связи.
18. Классификация методов защиты информации.
19. Правовые методы защиты информации.
20. Организационные методы защиты информации.
21. Экранирование узлов и соединений аппаратуры.
22. Снижение уровней наводок на проводные тракты и узлы аппаратуры.
23. Звукоизоляция помещений.
24. Акустическая маскировка.
25. Электромагнитная маскировка.
26. Технические средства обнаружения закладных устройств.
27. Методы поиска и классификация работ по обнаружению и подавлению закладных устройств.
28. Категорирование объектов.
29. Классификация инженерно-технических методов защиты информации.
30. Инженерные заграждения.
31. Технические средства охраны периметра.
32. Охранное телевидение.
33. Системы контроля и управления доступом.
34. Политика безопасности.
35. Механизмы защиты автоматизированных систем.
36. Принципы реализации политики безопасности.
37. Аутентификация.
38. Рекомендации по использованию устройств аутентификации.
39. Принципы криптографической защиты информации.

40. Алгоритм шифрования ГОСТ 28147-89. Режим простой замены.
41. Электронно-цифровая подпись.
42. Защита транзакций в Internet.
43. Интеллектуальная собственность в развитии общества.
44. Авторское право и смежные права.
45. Промышленная собственность.
46. Объекты и субъекты авторского права и смежных прав.
47. Патентная информация.
48. Патентные исследования.
49. Введение объектов интеллектуальной собственности в гражданский оборот.
50. Коммерческое использование объектов интеллектуальной собственности.
51. Защита прав авторов и правообладателей.
52. Государственное управление интеллектуальной собственностью.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Основные законы, стандарты и рекомендации в области информационной безопасности.
2. Модель нарушителя.
3. Угрозы безопасности информационных технологий.
4. Анализ и управление рисками.
5. Политика информационной безопасности.
6. Документы, регламентирующие политику безопасности организации.
7. Стандарты построения систем информационной безопасности.
8. Организация и функционирование службы информационной безопасности.
9. Поведение оценки и разработка планов обработки рисков информационной безопасности.
10. Обучение и повышение осведомленности в области информационной безопасности.
11. Мониторинг, контроль защитных мер и аудит информационной безопасности.
12. Анализ функционирования системы обеспечения информационной безопасности.
13. Создание системы защиты информации.
14. Подготовка и аттестация системы защиты информации.
15. Эксплуатация системы защиты информации.
16. Модернизация системы защиты информации.
17. Управление инцидентами в области информационной безопасности.
18. Угрозы сетевой безопасности.
19. Межсетевые экраны.
20. Системы обнаружения и предотвращения вторжений.

21. Виртуальные частных сети.

22. Классификация объектов, подлежащих охране с помощью технических средств охраны.

23. Основные принципы оборудования объектов техническими средствами охранной сигнализации.

24. Понятие уровней защиты объекта.

25. Понятие рубежей охранной сигнализации.

26. Принципы работы приборов приемно-контрольных.

27. Принципы работы охранных извещателей, оповещателей, КТС.

28. Назначение систем цифровой регистрации видеосигнала.

29. Принципы работы видеокамер и устройств хранения видеоинформации.

30. Назначение систем контроля и управления доступом.

31. Принципы работы идентификаторов доступа, исполнительных устройств и устройств хранения информации.

32. Основные требования к инженерно-технической укрепленности объектов различных форм собственности.

33. Классификация инженерных заграждений и их назначение.

34. Инженерная защита дверных проемов зданий и въездных ворот объекта.

V. ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разрабатывающей учебную программу (с указанием даты и номера протокола)
Метрология, стандартизация и сертификация (в информационных технологиях)	информационных технологий	нет	протокол заседания кафедры информационных технологий № 5 от 26.12.2024
Современные технологии обработки экономической информации	информационных технологий	нет	протокол заседания кафедры информационных технологий № 5 от 26.12.2024

I. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

ПРЕДМЕТ, СОДЕРЖАНИЕ И ЗАДАЧИ КУРСА, ЕГО МЕСТО В СИСТЕМЕ ПОДГОТОВКИ СПЕЦИАЛИСТА. ФОРМЫ ОТЧЕТНОСТИ

Современный человек находится в самой гуще информационного потока. Никогда в истории человечества не было такого объема данных, которые ежесекундно бы обрабатывал наш мозг. В этой динамичной среде важно создать для всех равные права в области обмена, поиска, получения и защиты информации.

Информационная безопасность (ИБ) – это совокупность методов по обеспечению целостности, неподдельности и конфиденциальности данных, а также пресечение их нецелевого использования.

Обеспечение любого мероприятия по ИБ всегда учитывает два понятия и оценивает эффективность мер исходя из ответов на вопросы:

Субъект информации – это любой владелец информации (человек, организация, государство).

Объект информации – объем данных любой сферы, которые необходимо защитить.

Всего существует три главных аспекта информационной безопасности (триада CIA). Они характеризуют параметры, которые должны быть обеспечены всеми элементами системы:

Триада CIA в ИТ – это как защита для данных: конфиденциальность не пускает чужих, целостность держит данные в порядке, а доступность гарантирует, что ты всегда можешь к ним добраться.

Триада CIA решает проблему защиты информации в интернете. Она как страж, который оберегает данные от воров (конфиденциальность), следит, чтобы никто не исказил информацию (целостность), и обеспечивает доступ к ним, когда это необходимо (доступность). Это основа, без которой невозможно обеспечить безопасность в сети.

Пример:

Вы владелец веб-сайта, который хранит важные данные пользователей.

Конфиденциальность: Вы используете SSL-сертификаты для шифрования данных, чтобы только авторизованные пользователи могли получить доступ к информации. Это как установка замка на дверь, чтобы никто посторонний не смог войти.

Целостность: Вы применяете системы контроля версий и регулярно делаете бэкапы, чтобы убедиться, что данные не будут изменены или удалены

неавторизованно. Это как проверка, что все вещи в вашем доме на месте и невредимы.

Доступность: Вы используете услуги облачного хостинга с высокой производительностью и защитой от DDoS-атак, чтобы ваш сайт всегда был доступен для пользователей. Это как убедиться, что вы всегда можете свободно войти и выйти из своего дома.

Таким образом, применение триады CIA в ИТ помогает защитить веб-сайт от несанкционированного доступа, неавторизованных изменений и обеспечивает постоянный доступ к нему для пользователей и владельцев. Это как построение и защита дома в цифровом мире.

Как обеспечить конфиденциальность информации

Конфиденциальность информации – это первый столп триады CIA. Это означает, что доступ к информации должен быть ограничен и предоставлен только тем, кто имеет на это право. Чтобы защитить данные в интернете от несанкционированного доступа, используются различные методы шифрования и аутентификации.

Примеры защиты конфиденциальности:

Шифрование: Преобразование данных в форму, которую нельзя прочитать без специального ключа. Это как отправка письма в непрозрачном конверте.

Аутентификация: Проверка личности пользователя перед предоставлением доступа к информации. Это как показать паспорт, прежде чем войти в защищенное здание.

Как поддерживать целостность данных

Целостность данных – это уверенность в том, что информация остается неповрежденной и актуальной. Это включает защиту от неавторизованных изменений, будь то случайные или преднамеренные.

Методы обеспечения целостности:

Контроль версий: Отслеживание изменений в документах или коде, чтобы можно было восстановить предыдущие версии при необходимости.

Цифровые подписи: Подтверждение подлинности документа или сообщения, что гарантирует, что содержимое не было изменено после подписания.

Как гарантировать доступность в ИТ

Доступность означает, что информация и ресурсы всегда доступны для тех, кто должен ими пользоваться. Это критически важно для бизнеса, где даже кратковременные перебои могут привести к значительным потерям.

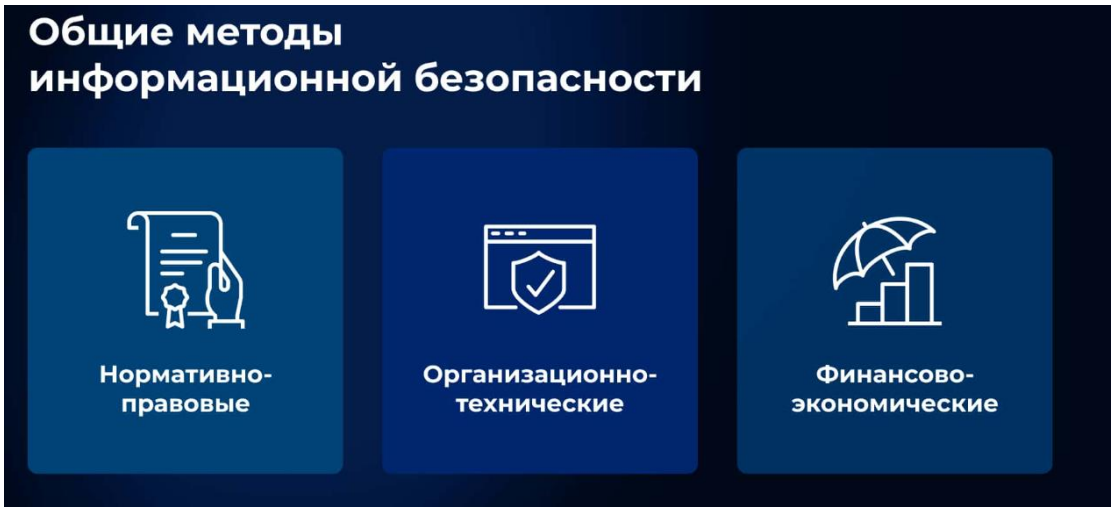
Способы обеспечения доступности:

Резервное копирование: Создание копий данных на случай сбоев или катастроф.

Защита от DDoS-атак: Применение мер для предотвращения атак, целью которых является сделать ресурс недоступным для его пользователей.

Общие методы обеспечения информационной безопасности

Методы ИБ делятся на три большие группы: нормативно-правовые, организационно-технические и финансово-экономические. Рассмотрим каждый из них подробнее.



1. Нормативно-правовые методы

Это фундамент. Методы заключаются в создании законов, указов и нормативных актов, которые устанавливают правила работы с информацией и ответственность за их нарушение.

Ключевой закон: Базовым документом является Закон Республики Беларусь «Об информации, информатизации и защите информации» (№ 455-З). Он определяет, что защите подлежит любая информация, неправомерные действия с которой могут причинить вред её владельцу.

Главное требование закона:

Информация с ограниченным доступом (не гостайна) и данные в государственных информационных системах должны обрабатываться с использованием аттестованной системы защиты информации. Проще говоря, если вы работаете с такими данными, ваша система защиты должна пройти официальную проверку и получить «сертификат качества».

Для этого можно использовать только сертифицированные в Беларуси средства защиты (программы и устройства). Они должны иметь сертификат Национальной системы подтверждения соответствия.

Деятельность по созданию средств защиты и реализации мер защиты подлежит лицензированию.

Права и обязанности: Закреплены также права и обязанности владельцев информации. Например, они обязаны обеспечивать защиту, контролировать её, а также иметь возможность незамедлительно восстановить информацию в случае её уничтожения или изменения.

2.Организационно-технические методы

Это самый обширный блок, включающий программные, аппаратные и процедурные меры защиты. Он решает три главные задачи: ограничение

физического доступа, предотвращение уничтожения носителей и защита от кражи данных.

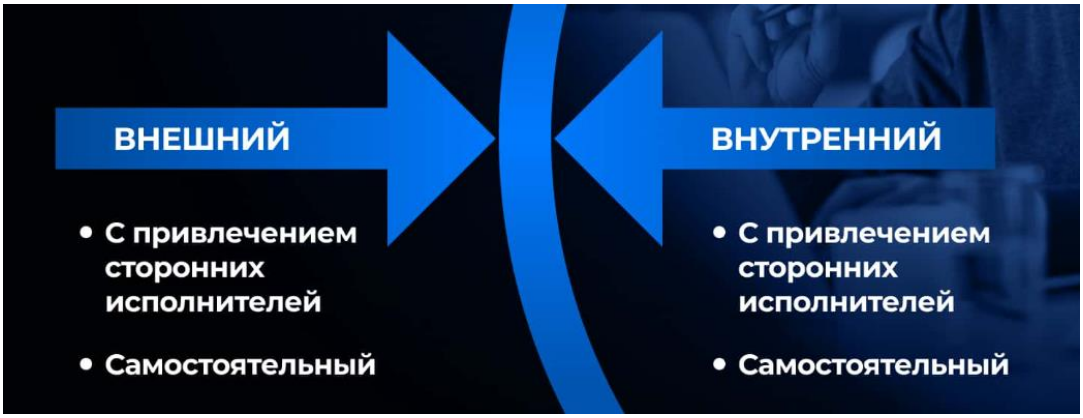
Инструменты защиты:

Программные: Антивирусы, DLP-системы (для защиты от утечек), SIEM-системы (мониторинг инцидентов).

Технические: СКУД (системы контроля доступа), видеонаблюдение, защищенные серверные.

Организационные: Регламенты, инструкции для персонала, политика паролей.

Важной частью является аудит ИБ – периодическая проверка эффективности защиты. Он может быть внешним (пентесты) или внутренним.



Финансово-экономические методы обеспечения информационной безопасности – это способы управления денежными потоками, инвестициями и рисками, направленные на создание эффективной и устойчивой системы защиты информации. Если правовые методы отвечают на вопрос «что нельзя делать?», а технические – «как защитить?», то экономические методы отвечают на вопрос «сколько это стоит и насколько это выгодно?»

Предметом изучения дисциплины являются теоретические и практические основы обеспечения информационной безопасности, методы и средства защиты информации, а также организационно-правовые механизмы, регламентирующие деятельность в этой сфере.

Структура курса включает три основных раздела (согласно учебной программе):

Основы информационной безопасности – формирование понятийного аппарата, социально-правовые аспекты, роль информации в современном обществе.

Угрозы и методы защиты информации в компьютерных системах – классификация угроз, эволюция концепций ИБ, повышение эксплуатационной надежности систем.

Организационное и комплексное обеспечение информационной безопасности – организационно-правовые механизмы, построение комплексных систем защиты информации (КСЗИ).

Такая структура позволяет последовательно перейти от общих теоретических вопросов к конкретным практическим методам и комплексным решениям.

В результате изучения дисциплины студент должен:

Знать:

нормативно-правовую базу в области информационной безопасности (законы, стандарты, технические кодексы);

организационно-технические методы и средства защиты информации;

классификацию угроз и модели нарушителей;

принципы построения комплексных систем защиты информации.

Уметь:

анализировать риски информационной безопасности;

проектировать и оценивать эффективность систем защиты;

применять нормативные требования при разработке политик безопасности.

Владеть навыками:

использования методов анализа защищенности объектов информатизации;

управления инцидентами информационной безопасности;

разработки организационно-распорядительной документации по защите информации.

ЗАЩИТА ИНФОРМАЦИИ КАК ОБЪЕКТИВНАЯ ЗАКОНОМЕРНОСТЬ ЭВОЛЮЦИИ ПОСТИНДУСТРИАЛЬНОГО ОБЩЕСТВА. ИНФОРМАЦИЯ И ЕЕ РОЛЬ В СОВРЕМЕННОМ ОБЩЕСТВЕ

«Кто владеет информацией, тот владеет миром» (Н. Ротшильд).

Современный этап развития человечества характеризуется фундаментальными изменениями в структуре экономики, социальных отношений и самой природе производства. Для понимания того, почему защита информации становится объективной необходимостью, а не просто технической задачей, необходимо рассмотреть эволюцию общества через призму смены технологических укладов.

Концепция постиндустриального общества, разработанная Дэниелом Беллом, Элвином Тоффлером и другими исследователями во второй половине XX века, оказалась пророческой. Сегодня мы наблюдаем завершение перехода развитых стран к новой стадии развития, где информация и знания становятся главным стратегическим ресурсом.

Три стадии цивилизационного развития

1. Доиндустриальное (аграрное) общество

На протяжении тысячелетий основой экономики было сельское хозяйство. Главным ресурсом выступала земля, а основным фактором производства – физический труд. Производительность труда оставалась низкой, общество было жестко структурировано, а социальная мобильность – минимальной. Энергетической основой служила мускульная сила человека и животных.

1. Индустриальное общество

Промышленная революция XVIII-XIX веков коренным образом изменила мир. На смену земле пришел капитал, основным типом производства стало изготовление товаров на фабриках и заводах. Ключевую роль сыграли энергетические ресурсы – сначала уголь, затем нефть и электричество. Общество стало массовым, стандартизированным, с высокой социальной мобильностью, но и с острыми классовыми противоречиями между трудом и капиталом.

Количественные показатели индустриальной эпохи:

Рост производительности труда в 50-100 раз по сравнению с аграрным обществом

Урбанизация: доля городского населения в развитых странах выросла с 10-15% до 70-80%

Снижение доли занятых в сельском хозяйстве до 2-5%.

2. Постиндустриальное общество: качественный скачок

С середины XX века в развитых странах формируется общество нового типа. Его принципиальное отличие – переход от взаимодействия человека с преобразованной природой к взаимодействию между людьми по поводу информации и знаний.

Ключевые характеристики постиндустриального общества

Если в индустриальную эпоху богатство создавалось за счет контроля над материальными ресурсами (нефть, сталь, станки), то в постиндустриальном обществе главным источником стоимости становится информация. Наиболее успешные компании современности – Google, Microsoft, Apple – торгуют не материальными продуктами, а информацией и знаниями, воплощенными в программном обеспечении и сервисах.

Как отмечает британский социолог Фрэнк Уэбстер, ключевым признаком информационного общества становится не просто обилие информации, а превращение теоретического знания в непосредственную производительную силу. Это означает, что:

Инновации возникают не случайно, а как результат целенаправленных научных исследований.

Высшее образование становится массовым (в развитых странах до 60-70% молодежи получает высшее образование).

Расходы на НИОКР составляют значительную часть ВВП (2.5-3.5% в США, Германии, Японии, Южной Корее).

Информационное общество организуется не иерархически (как армия или бюрократия), а сетевым образом. Горизонтальные связи становятся важнее вертикальных. Это проявляется в:

Децентрализации бизнес-структур.

Развитии аутсорсинга и распределенных команд.

Возникновении платформенных компаний (Uber, Airbnb), которые сами не производят товары, а организуют взаимодействие между участниками рынка.

Для понимания того, почему информация требует особых механизмов защиты, необходимо осознать ее фундаментальные отличия от материальных ресурсов.

Материальные ресурсы (нефть, уголь, металлы) конечны. Их потребление уменьшает доступный запас. Информация же обладает принципиально иным свойством: при потреблении она не убывает, а может даже возрастать. Когда вы делитесь знанием, у вас его не становится меньше. Более того, в процессе обсуждения и обмена знание может углубляться и обогащаться.

Исследования показывают прямую связь между уровнем информатизации общества и его экономическим развитием. Наиболее доступным и общеизвестным показателем, отражающим качество человеческого капитала, является Индекс человеческого развития (ИЧР), который включает:

Ожидаемую продолжительность жизни.

Уровень образования.

Валовой национальный доход на душу населения.

Страны с высоким уровнем информатизации (Норвегия, Швейцария, Ирландия, Германия, Сингапур) стабильно занимают верхние строчки рейтинга ИЧР.

На современном этапе информационная сфера стала системообразующим фактором общественной жизни. Это означает, что:

Без постоянного информационного обмена невозможно функционирование ни одной социальной группы.

Средства массовой информации формируют общественное мнение и повестку дня.

Государственная политика реализуется через информационное обеспечение.

Из всего вышесказанного следует ключевой для нашего курса вывод: информация стала стратегическим ресурсом, от сохранности и качества которого зависит функционирование всех сфер общества.

Это порождает объективную необходимость защиты информации:

экономическая ценность – информация имеет стоимость, ее утрата или хищение наносят ущерб;

политическое значение – доступ к информации определяет властные отношения;

социальная роль – защита персональных данных обеспечивает права личности;

технологическая зависимость – современные инфраструктуры уязвимы для кибератак.

Постиндустриальное общество знаменует собой принципиально новый этап развития человечества, где информация становится главным ресурсом, а знания – основной производительной силой. Это порождает как новые возможности (ускорение научно-технического прогресса, персонализация услуг, глобальная коммуникация), так и новые вызовы (цифровое неравенство, уязвимость инфраструктур, необходимость защиты информации).

Понимание этих процессов необходимо для осознания того, почему вопросы информационной безопасности выходят за рамки узкотехнических и становятся стратегическими для бизнеса, государства и каждого человека.

Однако в век такой высокой скорости информатизации и проблемы часто существуют: влияние информационных технологий на социальное развитие имеет как «плюсы», так и «недостатки».

С появлением и популяризацией интернета, а также развитием и прогрессом информационных технологий скорость обучения людей возрастает, и влияние информации на общество перекрывает очень важную позицию, количество информации, скорость распространения информации, скорость обработки информации и применения информации. Скорость быстро увеличивается, что не только способствует повышению эффективности труда людей, улучшает качество жизни, но также способствует техническому прогрессу и ускоряет промышленные преобразования.

Человечество вступает в информационную эпоху из индустриальной эпохи. После вступления в 21 век информация становится первым фактором производства, а также важной технической и материальной основой информационного общества. 21 век стал веком информации.

Информатизация – это новый этап, возникающий в результате продвижения человеческого общества к определенному этапу. Он основан на передовых технологиях, таких как компьютерные технологии, цифровые технологии и биоинженерные технологии. Получить и реализовать все достижения цивилизации, созданные человечеством, и предоставить человечеству очень эффективные средства связи, способствовать тесному обмену и диалогу между народами всех стран мира, укрепить взаимопонимание и принести пользу общему процветанию человечества.

Информационный век сближает общество, но он также создает множество проблем, открывая возможности для человечества. В эпоху информатизации интернета количество социальной информации резко возросло, скорость потока увеличивалась, и информация начала переполняться, что не только превышает способность людей обрабатывать и использовать информацию, но и заставляет людей испытывать чрезмерные страдания. информационные шоки.

В тоже время начали появляться огромные количества бесполезной информации, вредной информации и информации, наносящей вред всем аспектам человеческого общества, что создает угрозу безопасному применению и распространению информации. Могут даже возникать такие проблемы, как нарушение безопасности сети, кража данных и утечка информации, что может спровоцировать киберпреступления. Чем выше популярность Интернета, тем больше вреда от киберпреступности.

Киберпреступность процветает не только из-за технологий, но и из-за человеческого фактора – отсутствия ощущения кризиса у пользователей и бизнеса, которые пренебрегают базовыми правилами гигиены безопасности.

Сегодня, в век информации, с быстрым развитием экономики и технологий, количество рабочих мест постепенно сокращается, а конкуренция в

информационном обществе становится все более ожесточенной. Популярность века информации меняется в любое время, и эту тенденцию невозможно остановить. Если законы и тенденции экономического развития невозможно понять вовремя, они должны быть устранены обществом. Следовательно, только осознавая направление развития рыночной экономики, мы можем воспользоваться моментом и двигаться по правильному пути.

В настоящее время многие страны мира выдвинули свои собственные стратегии информатизации, активно развивают и продвигают применение информационных технологий, которые не только способствуют развитию человечества, но и помогают улучшить качество жизни людей. Развитие информационных технологий – это путь к сильной стране, и развитие информационных технологий также является неиссякаемой движущей силой прогресса различных стран.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА: СОЦИАЛЬНО-ПРАВОВЫЕ АСПЕКТЫ

В настоящее время происходит не только значительный рост количества и качества информационных ресурсов, но и выброс в информационное пространство избыточной, во многом искаженной и недостоверной информации.

Все это обостряет проблему обеспечения информационной безопасности личности и делает ее исключительно злободневной и актуальной.

Безопасность личности – состояние защищенности ее жизненно важных интересов (совокупность потребностей, удовлетворение которых обеспечивает существование и возможность прогрессивного развития личности) от внутренних и внешних угроз.

Принципы информационной безопасности призваны обеспечить удовлетворение информационных потребностей человека и его безопасное существование в информационной среде.

Опасным источником угроз интересам личности является использование во вред его персональных данных, накапливаемых различными структурами, а также расширение возможности скрытого сбора личной информации, сведений о частной жизни.

Одной из составляющих жизненно важных интересов человека в информационном пространстве является потребность быть огражденным от ложной, дефектной, фальсифицированной и другой вредной информации, представляющей угрозу для его существования и прогрессивного развития. Удовлетворение этих потребностей является конституционным правом каждого человека и гражданина при условии, что это право осуществляется законным способом.

Воспрепятствование удовлетворению законных информационных интересов человека представляет собой угрозу его информационной безопасности. В связи с этим особое значение приобретает ответственное поведение всех участников информационных процессов, а также выработка общих правил коммуникации в

информационном пространстве, основанных на признании идентичности прав и обязанностей в существующей реальности (физическом мире) и виртуальном пространстве.

В нашей стране разработана «Концепция информационной безопасности Республики Беларусь», которая обеспечивает комплексный подход к проблеме информационной безопасности.

В концепции вопрос обеспечения информационной безопасности рассматривается как система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз.

Основной целью государственной политики в области обеспечения безопасности информационных ресурсов является сохранение их доступности, целостности и конфиденциальности.

Актуальным является вопрос защиты персональных данных.

К основным персональным данным относятся: фамилия, собственное имя, отчество, пол, число, месяц, год рождения, место рождения, данные о гражданстве (подданстве), цифровой фотопортрет, данные о регистрации по месту жительства и (или) месту пребывания, данные о смерти или объявлении физического лица умершим, признании безвестно отсутствующим, недееспособным, ограниченно дееспособным.

Дополнительные персональные данные – данные о родителях, опекунах, попечителях, семейном положении, супруге, ребенке (детях) физического лица, о высшем образовании, ученой степени, ученом звании, о роде занятий, налоговых обязательствах.

К личной тайне могут быть отнесены сведения, использование которых без согласия заинтересованных лиц может нанести ущерб моральным и имущественным интересам граждан, в их числе: сведения о здоровье, семейных отношениях; об обстоятельствах рождения, усыновления, развода; сведения о личных привычках и наклонностях; личная переписка и корреспонденция, дневниковые, телефонные, телеграфные, видео, аудио и другие виды сохранения информации; сведения об имущественном положении, источниках доходов; о деятельности, содержащей коммерческую тайну; об интеллектуальной собственности (авторское право, изобретательское и патентное право, право на научные открытия); сведения, разглашение которых создает угрозу личной безопасности граждан, безопасности членов их семей и имущества; об участии граждан в действиях судебно-следственных органов в качестве свидетелей и т. д., а также об обвинении в злоупотреблениях властью или служебным положением и др.

Основы правовой защиты личной информации заложены в статье 28 Конституции Республики Беларусь, согласно которой каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну корреспонденции, телефонных и иных сообщений, на честь и достоинство.

Согласно статье 27 Конституции Республики Беларусь, никто не должен принуждаться к даче показаний и объяснений против самого себя, членов семьи или близких родственников. Доказательства, полученные с нарушением закона, не имеют юридической силы.

Персональные данные, проходящие автоматическую обработку, должны быть:

• получены и обработаны добросовестным и законным образом;

• сохранены для точно определенных и законных целей и не могут использоваться в противоречии с этими целями;

• адекватными, относящимися к делу и не избыточными применительно к целям, для которых они накапливаются;

• точными и в случае необходимости обновляемыми;

• сохраненными в такой форме, которая позволяет идентифицировать субъектов данных не дольше, чем этого требует цель, для которой соответствующие данные накапливаются.

Информационные процессы не ограничиваются взаимодействием на уровне отдельного человека. Интегрируясь в социальные группы и институты, личность участвует в формировании коллективных представлений, ценностных ориентаций и моделей поведения, которые составляют основу функционирования общества в целом.

В этом контексте угрозы, ранее рассматриваемые как индивидуальные (получение ложной информации, манипуляция сознанием), приобретают системный характер. Дезинформация, распространяясь в социальных сетях и медиа, способна влиять на общественное мнение, подрывать доверие к социальным институтам и провоцировать социальную напряженность. Деструктивная пропаганда может трансформировать ценностную структуру общества, а распространение экстремистских идей – создавать прямые угрозы общественной безопасности.

Таким образом, от анализа безопасности личности необходимо перейти к рассмотрению информационной безопасности общества. В научной литературе данное понятие определяется как состояние защищенности общественных отношений, общественного сознания и системы социальных норм от информационных угроз, способных нарушить стабильность функционирования социума и его прогрессивное развитие. Ключевыми объектами защиты здесь выступают не персональные данные, а коллективные представления, социальное доверие и ценностный консенсус.

Дезинформация и ее воздействие на социальные процессы

В современном информационном обществе дезинформация представляет собой не просто совокупность ложных сведений, а целенаправленно конструируемый информационный продукт. Его отличительной чертой является наличие субъекта (актора), преследующего определенные цели, и использование каналов массовой коммуникации для воздействия на широкую аудиторию.

Социальные последствия распространения дезинформации:

1. Снижение уровня социального доверия. Регулярное столкновение с противоречивой и заведомо ложной информацией ведет к эрозии доверия к социальным институтам, призванным производить и верифицировать знания: науке, образованию, журналистике, органам государственного управления. Формируется феномен «постправды», при котором эмоционально окрашенные убеждения начинают доминировать над объективными фактами в процессе формирования общественных мнений и оценок.

2. Социальная фрагментация. Алгоритмические системы современных цифровых платформ, ориентированные на удержание внимания пользователя, способствуют формированию замкнутых информационных пространств («информационных пузырей»). Внутри таких пространств циркулирует преимущественно однотипная информация, подтверждающая уже сложившиеся взгляды. Дезинформация, попавшая в такой «пузырь», многократно усиливается, что ведет к поляризации общества и затруднению диалога между различными социальными группами.

3. Дестабилизация социальной обстановки. Информационные вбросы, моделирующие ситуации дефицита, угрозы здоровью или социальной несправедливости, могут выступать катализаторами панических настроений, ажиотажного спроса или стихийных массовых акций. В данном случае дезинформация выполняет функцию дестабилизирующего фактора, нарушающего нормальное течение социальных процессов.

Деструктивная пропаганда как инструмент трансформации ценностей

Пропаганда в широком смысле представляет собой деятельность по распространению знаний, взглядов и идей с целью формирования определенных мировоззренческих установок. В зависимости от направленности она может выполнять как конструктивные (просвещение, популяризация здорового образа жизни), так и деструктивные функции. Деструктивная пропаганда ориентирована на внедрение в массовое сознание идей и ценностей, противоречащих интересам устойчивого развития общества.

Основные направления и методы деструктивного пропагандистского воздействия:

Ценностная дезориентация. Данный механизм предполагает постепенную подмену традиционных для данного общества ценностей (созидательный труд, коллективизм, взаимопомощь, патриотизм) на альтернативные модели (крайний индивидуализм, гедонизм, потребительство, циничное отношение к истории и культуре). Результатом такой дезориентации становится размывание ценностного консенсуса, необходимого для поддержания социальной солидарности.

Легитимизация девиантных форм поведения. Через многократную репрезентацию в медиапространстве образцов агрессивного, асоциального или аморального поведения как привлекательных или «нормальных» происходит постепенное смещение общественных представлений о границах допустимого. Снижается порог чувствительности к нарушениям социальных норм, что в

долгосрочной перспективе ведет к росту соответствующих форм поведения в обществе.

Дискредитация социальных институтов. Системное формирование негативного образа государственных органов, системы образования, здравоохранения, судебной власти подрывает авторитет этих институтов. Следствием становится снижение эффективности их функционирования, так как доверие является необходимым условием для выполнения институтами своих социальных функций.

Эмоциональное манипулирование. В отличие от рациональной аргументации, деструктивная пропаганда часто апеллирует к базовым эмоциям – страху, гневу, чувству несправедливости. Использование ярких образов, упрощенных лозунгов и приемов «навешивания ярлыков» блокирует критическое восприятие информации и облегчает внедрение нужных установок.

Информационный экстремизм: природа и каналы распространения

Экстремизм как социальное явление представляет собой приверженность крайним взглядам и методам действия, направленным на дестабилизацию общественного порядка, разжигание розни или насильственное изменение основ конституционного строя. Информационный экстремизм является специфической формой данного явления, реализуемой через производство и распространение соответствующего контента в информационном пространстве.

Цифровая среда создает благоприятные условия для функционирования экстремистских структур благодаря следующим факторам:

Возможность анонимного присутствия, затрудняющая идентификацию авторов противоправных материалов.

Высокая скорость распространения контента, позволяющая оперативно охватывать значительную аудиторию.

Наличие механизмов таргетирования, дающих возможность адресовать информацию тем категориям пользователей, которые наиболее восприимчивы к радикальной идеологии (например, молодежи в кризисных жизненных ситуациях).

Социальные функции информационного экстремизма:

Рекрутинговая функция. Создание привлекательного имиджа радикальных групп, трансляция их идеологии и последующая психологическая обработка потенциальных сторонников через закрытые коммуникационные каналы.

Координационная функция. Использование защищенных каналов связи (мессенджеров, закрытых групп) для согласования противоправных действий без риска оперативного обнаружения.

Функция психологического давления. Распространение контента, содержащего сцены насилия или угрозы, с целью деморализации оппонентов и подавления воли к сопротивлению у широкой общественности.

Функция конструирования образа врага. Формирование в массовом сознании устойчивого представления об определенной социальной, этнической или религиозной группе как источнике угроз, что служит идеологическим обоснованием для агрессии в ее адрес.

Система противодействия информационным угрозам

Обеспечение информационной безопасности общества требует применения комплексного подхода, интегрирующего правовые, организационно-технические и социально-воспитательные механизмы.

Правовой блок мер включает разработку и совершенствование нормативной базы, устанавливающей ответственность за распространение дезинформации, экстремистских материалов и деструктивной пропаганды. Важным аспектом является правовое регулирование деятельности интернет-платформ, обеспечивающее соблюдение национального законодательства на территории страны. Правовые нормы должны быть четко сформулированы, чтобы исключить их произвольное толкование, и обеспечивать неотвратимость наказания за нарушения.

Организационно-технический блок мер предполагает создание и поддержание функционирования систем мониторинга информационного пространства. Задача таких систем – своевременное выявление деструктивного контента и угроз его массового распространения. На основе данных мониторинга принимаются решения о блокировке опасных ресурсов или ограничении доступа к ним. Кроме того, важным направлением является развитие национальных систем проверки достоверности информации (фактчекинга), предоставляющих гражданам инструменты для верификации получаемых сведений.

Социально-воспитательный блок мер носит стратегический характер, поскольку направлен на формирование у населения долговременного иммунитета к деструктивным информационным воздействиям. Ключевые направления данного блока:

Развитие медиаграмотности и критического мышления. Внедрение в образовательные программы различных уровней модулей, обучающих методам проверки источников информации, распознавания манипулятивных техник, различения фактов и их интерпретаций.

Поддержка национально-культурной идентичности. Трансляция и популяризация знаний об истории, культуре и традициях, формирующих чувство принадлежности к единому социальному целому. Устойчивая идентичность снижает восприимчивость к внешним попыткам ценностной дезориентации.

Формирование позитивного информационного пространства. Создание и распространение контента, ориентированного на социально одобряемые модели поведения, традиционные ценности, созидательную деятельность. Насыщение информационной среды качественным и полезным контентом естественным образом вытесняет контент деструктивный.

Общество как совокупность индивидов и социальных групп существует в организованных формах, важнейшей из которых выступает государство. Государство является институтом, обеспечивающим суверенитет,

территориальную целостность, правопорядок и условия для устойчивого развития на определённой территории. В условиях цифровой трансформации и глобализации информационных процессов государство само становится объектом информационных угроз качественно иного уровня.

Информационная безопасность государства представляет собой составную часть национальной безопасности. Её обеспечение направлено на защиту суверенитета, территориальной целостности, политической, экономической и военной стабильности страны от угроз, реализуемых в информационном пространстве. В отличие от безопасности личности и общества, где акцент делается на правах и ценностях, безопасность государства фокусируется на сохранности информационных ресурсов, имеющих стратегическое значение, и непрерывности функционирования государственных систем управления и инфраструктуры.

Для Республики Беларусь, как и для большинства современных государств, характерно расширение спектра информационных угроз. Согласно положениям Концепции информационной безопасности Республики Беларусь, к числу основных угроз в государственной сфере относятся:

проведение специальных информационных операций, направленных против государства;

техническая разведка и несанкционированный доступ к государственным секретам;

кибератаки на объекты критической инфраструктуры;

использование информационных технологий для дестабилизации политической обстановки.

Защита государственной тайны

Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб национальной безопасности. В Республике Беларусь правовую основу защиты гостайны составляют Закон «О государственных секретах», а также ряд подзаконных актов, регламентирующих порядок отнесения сведений к гостайне, их засекречивания и рассекречивания.

Основные направления защиты гостайны:

1. Классификация и категорирование сведений. Определяются уровни секретности («особой важности», «совершенно секретно», «секретно») и устанавливаются правила доступа должностных лиц к таким сведениям.

2. Режим секретности на объектах. В государственных органах и организациях, работающих с секретными документами, создаются специальные подразделения (режимно-секретные органы), контролирующие порядок хранения, передачи и уничтожения носителей гостайны.

3. Защита от технической разведки. Применяются средства криптографической защиты, экранирования помещений, антивирусного и антиперехватного оборудования. Особое внимание уделяется защите каналов связи, по которым передаются секретные данные.

4. Работа с кадрами. Граждане, допускаемые к гостайне, проходят проверочные мероприятия, дают подписку о неразглашении и предупреждаются об ответственности за её утрату или разглашение.

Обеспечение обороноспособности в информационной сфере

Информационная составляющая обороноспособности государства включает два аспекта: во-первых, защиту собственных информационных систем военного назначения, и во-вторых, способность парировать информационные операции, направленные против вооружённых сил и населения.

Структура информационной безопасности оборонного сектора:

Защита автоматизированных систем управления войсками и оружием. Современные вооружённые силы используют цифровые каналы связи и системы управления, которые могут стать целью кибератак. Нарушение их работы способно дезорганизовать управление частями и применение средств поражения. В связи с этим принимаются меры по резервированию каналов, использованию защищённых протоколов и регулярному тестированию на проникновение.

Информационное обеспечение военной деятельности. Включает сбор, обработку и анализ данных об обстановке, а также доведение достоверной информации до личного состава и населения. Создание системы оперативного информирования позволяет противодействовать слухам и дезинформации в войсках.

Противодействие информационно-психологическим операциям. Специальные структуры Вооружённых сил и органов госбезопасности отслеживают попытки воздействия на сознание военнослужащих и гражданского населения через СМИ и интернет, разрабатывают контрмеры и ведут разъяснительную работу.

Подготовка кадров. В военных учебных заведениях Республики Беларусь (например, на факультетах связи и АСУ) готовятся специалисты по кибербезопасности и защите информации.

Важно отметить, что обеспечение обороноспособности в информационной сфере осуществляется в тесной координации с органами государственной безопасности и Оперативно-аналитическим центром при Президенте Республики Беларусь.

Защита критической информационной инфраструктуры

Критическая инфраструктура представляет собой комплекс объектов и систем, которые играют ключевую роль в обеспечении жизнедеятельности государства и общества в целом. В Республике Беларусь к критической

инфраструктуре относятся не только энергетическая система, транспортные сети, связь, финансовые учреждения и здравоохранение, но и такие важные элементы, как управление воздушным движением, системы водоснабжения и канализации, а также учреждения, обеспечивающие безопасность и правопорядок. Нарушение работы этих систем может привести к серьезным последствиям, включая угрозу безопасности, экономическим потерям и дестабилизации общественной жизни.

Защита критической инфраструктуры от кибератак становится особенно актуальной в условиях современного мира, где киберугрозы постоянно эволюционируют и становятся все более сложными. В Беларуси для обеспечения безопасности этих объектов и систем принимаются комплексные меры. Во-первых, разрабатываются и внедряются стандарты информационной безопасности, которые учитывают специфические риски и угрозы, характерные для каждого сектора критической инфраструктуры. Это включает в себя создание четких протоколов реагирования на инциденты и регулярное обновление программного обеспечения.

Во-вторых, проводятся регулярные аудиты и тестирования систем безопасности, что позволяет выявлять уязвимости и оперативно их устранять. Эти мероприятия помогают не только поддерживать высокий уровень безопасности, но и повышать общий уровень осведомленности о киберугрозах среди сотрудников.

Обучение персонала является еще одной важной составляющей кибербезопасности. Специалисты проходят тренинги, на которых знакомятся с актуальными методами защиты информации, а также с новейшими киберугрозами. Это позволяет не только улучшить навыки работы с информационными системами, но и формировать культуру безопасности в организациях.

Кроме того, создаются резервные системы и планы восстановления, которые позволяют минимизировать последствия в случае кибератаки. Эти планы включают в себя не только технические решения, но и организационные меры, такие как распределение ролей и обязанностей в кризисных ситуациях.

Взаимодействие с международными организациями также играет важную роль в обеспечении кибербезопасности. Беларусь активно участвует в обмене информацией и опытом с другими странами, что позволяет адаптировать лучшие практики и технологии для защиты своей критической инфраструктуры. Это сотрудничество включает в себя участие в международных учениях и конференциях, что способствует повышению квалификации специалистов и укреплению международных связей в области киберзащиты.

Таким образом, комплексный подход к защите критической инфраструктуры в Беларуси включает в себя разработку стандартов, регулярные проверки, обучение персонала, создание резервных систем и международное сотрудничество.

Это позволяет не только обеспечивать безопасность ключевых объектов, но и повышать устойчивость государства к киберугрозам в целом.

Беларусь активно наращивает усилия по обеспечению национальной кибербезопасности, понимая её критическую роль в поддержании стабильности государства и функционировании критически важной инфраструктуры. Ключевым направлением является создание единого центра мониторинга и реагирования на кибератаки. Этот центр, помимо сбора и анализа информации о киберугрозах в режиме реального времени, будет играть роль координационного узла, объединяющего усилия различных государственных органов, предприятий критической инфраструктуры и частного сектора. Планируется, что центр будет оснащен передовыми технологиями анализа данных, искусственным интеллектом для выявления аномалий и прогнозирования угроз, а также системой быстрого реагирования на инциденты, позволяющей минимизировать ущерб от кибератак. Его создание требует значительных инвестиций в высококвалифицированные кадры, современное оборудование и программное обеспечение, а также тесную интеграцию с международными партнерами для обмена разведданными.

Международное сотрудничество является неотъемлемой частью белорусской стратегии кибербезопасности. Активно развиваются двусторонние отношения с рядом стран, в рамках которых проводятся обмены опытом, совместные тренировки и разработка соглашений о взаимной помощи в случае кибератак. Особое внимание уделяется сотрудничеству в рамках Организации Договора о коллективной безопасности (ОДКБ). В рамках ОДКБ проводятся масштабные совместные учения, симулирующие различные сценарии кибератак на объекты критической инфраструктуры, государственные органы и финансовые институты.

Эти учения позволяют отработать взаимодействие между различными службами безопасности государств-членов, совершенствовать методы обнаружения и реагирования на угрозы, а также обмениваться актуальной информацией о новых типах вредоносных программ и тактиках киберпреступников. Кроме того, в рамках ОДКБ разрабатываются общие стандарты кибербезопасности, правовые основы сотрудничества и механизмы взаимной поддержки.

Беларусь активно участвует в деятельности международных организаций, таких как Международный телекоммуникационный союз (МТСС), Международный союз электросвязи (МСЭ), а также в работе специализированных комитетов ООН и других международных форумов по кибербезопасности. Это позволяет не только быть в курсе последних тенденций в области киберугроз и лучших мировых практик, но и вносить свой вклад в разработку международных стандартов и норм в сфере кибербезопасности. Участие в таких организациях способствует обмену опытом с ведущими экспертами мирового уровня, содействует развитию национальной нормативно-правовой базы и позволяет получать доступ к передовым технологиям и решениям в области защиты от киберугроз.

Однако, перед Беларусью стоят серьезные вызовы. Быстрое развитие искусственного интеллекта, расширение использования Интернета вещей (IoT) и появление новых, более изощренных методов кибератак, таких как атаки с использованием квантовых компьютеров и целенаправленные атаки на основе искусственного интеллекта (AI-driven attacks), требуют постоянного совершенствования стратегии кибербезопасности. Необходимо постоянно адаптироваться к изменяющейся глобальной обстановке, учитывая растущую роль киберпространства в геополитических процессах и потенциальные угрозы со стороны государственных и негосударственных акторов. Это требует значительных инвестиций в научные исследования и разработки в области кибербезопасности, постоянное повышение квалификации специалистов и внедрение современных технологий защиты информации.

КОМПЬЮТЕРНАЯ СИСТЕМА КАК ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

На предыдущих лекциях мы установили, что информация – это ценный ресурс, который нуждается в защите. Но информация не существует в вакууме. В современном мире она создается, хранится, обрабатывается и передается с помощью компьютерных систем (КС). Следовательно, чтобы защитить информацию, мы должны защищать ту среду, в которой она находится. Таким образом, компьютерная система становится непосредственным объектом защиты.

Определение: Компьютерная система (информационная система) с точки зрения информационной безопасности – это совокупность взаимосвязанных компонентов, включающая аппаратное и программное обеспечение, данные, персонал и поддерживающую инфраструктуру, предназначенная для автоматизации процессов работы с информацией.

Защита КС требует комплексного, эшелонированного (многоуровневого) подхода, поскольку уязвимость любого из ее компонентов может привести к компрометации всей системы.

1. Аппаратное обеспечение (Hardware):

– Состав: Серверы, рабочие станции, сетевое оборудование (маршрутизаторы, коммутаторы), периферийные устройства, носители информации (HDD, SSD).

–Что защищаем: Физическую целостность и доступность оборудования. Защита от кражи, повреждения, несанкционированного физического доступа.

2. Программное обеспечение (Software):

– Состав:

– Системное ПО: Операционные системы (Windows, Linux), системы управления базами данных (СУБД), драйверы.

– Прикладное ПО: Офисные пакеты, бухгалтерские программы, ERP-системы, веб-браузеры.

– Что защищаем: Целостность кода, корректность функционирования, защиту от эксплуатации уязвимостей.

3. Информационные ресурсы (Данные):

– Состав: Файлы, базы данных, архивы, конфигурационные файлы, учетные данные пользователей (логины/пароли).

– Что защищаем: Это и есть конечная цель защиты. Обеспечиваем триаду ИБ: конфиденциальность, целостность и доступность самой информации.

4. Персонал (Пользователи и обслуживающий персонал):

– Состав: Системные администраторы, разработчики, операторы, конечные пользователи.

– Что защищаем/от чего защищаемся: Человеческий фактор. Защита от непреднамеренных ошибок (случайное удаление данных), а также от преднамеренных действий инсайдеров (слив информации, саботаж).

5. Физическая среда и поддерживающая инфраструктура:

− Состав: Помещения (серверные), системы электропитания, кондиционирования, линии связи.

− Что защищаем: Обеспечение стабильных условий для функционирования аппаратного обеспечения.

Защита КС – это не просто установка антивируса. Это комплекс мер, направленных на каждый из пяти перечисленных компонентов.

Определение: Угроза информационной безопасности – это потенциально возможное событие, действие или процесс, которое может нанести ущерб информационным ресурсам и компонентам компьютерной системы.

Угрозы реализуются через уязвимости. Уязвимость – это недостаток в системе, который делает возможной реализацию угрозы.

Классификация угроз:

2.1. По источнику возникновения:

−Естественные угрозы: Вызваны стихийными бедствиями (пожар, наводнение, ураган). Не зависят от человека.

− Последствия: Физическое уничтожение оборудования, потеря доступности информации.

− Искусственные (антропогенные) угрозы: Вызваны деятельностью человека. Являются основным предметом изучения ИБ. Делятся на:

− Непреднамеренные (случайные): Ошибки пользователей и персонала (случайное удаление файла, ввод неверных данных), сбои ПО и оборудования, неправильная конфигурация систем.

−Преднамеренные (умышленные): Целенаправленные действия нарушителей (внутренних или внешних) с целью нанесения ущерба. Это и есть атаки.

2.2. По воздействию на основные свойства информации (триаду ИБ):

− Угрозы конфиденциальности (нарушение секретности): Направлены на несанкционированное получение доступа к защищаемой информации.

− Примеры: Кража паролей, перехват сетевого трафика (сниффинг), несанкционированный доступ к файлам, социальная инженерия (фишинг).

− Угрозы целостности (нарушение достоверности): Направлены на несанкционированное изменение или уничтожение информации.

−Примеры: Внедрение вредоносного ПО (вирусы, которые портят файлы), подмена данных в базах данных, фальсификация сообщений (спуфинг).

−Угрозы доступности (отказ в обслуживании): Направлены на блокирование доступа легитимных пользователей к ресурсам КС.

−Примеры: DoS/DDoS-атаки (перегрузка сервера запросами), шифрование данных с целью выкупа (Ransomware), физическое уничтожение оборудования.

2.3. По типу (способу реализации) преднамеренных атак:

Тип угрозы/атаки	Цель (что нарушает)	Краткое описание и пример
Несанкционированный доступ (НСД)	Конфиденциальность, Целостность	Получение доступа к системе или данным в обход правил разграничения доступа. *Пример: подбор пароля, эксплуатация уязвимости в ПО.*
Вредоносное ПО (Malware)	Все три свойства	Программы, созданные для нанесения вреда КС. *Примеры:* **Вирусы** *(портят файлы),* **Трояны** *(скрытно выполняют вредные действия),* **Шифровальщики (Ransomware)** *(блокируют доступ к данным).*
Отказ в обслуживании (DoS/DDoS)	Доступность	Отправка огромного количества запросов на сервер с целью его перегрузки и вывода из строя. DDoS – атака с множества компьютеров.
Социальная инженерия	Конфиденциальность	Психологическая манипуляция людьми с целью получения конфиденциальной информации (паролей, данных карт). *Пример:* **Фишинг** – *рассылка поддельных писем от имени банков или соцсетей.*
Перехват данных (Sniffing)	Конфиденциальность	"Прослушивание" сетевого трафика для получения незашифрованных данных (логинов, паролей).
Подмена (Spoofing)	Целостность	Фальсификация данных (например, IP-адреса или email-адреса отправителя), чтобы выдать себя за другого субъекта.

Компьютерная система – это многокомпонентный объект защиты, и безопасность может быть обеспечена только при комплексном подходе, учитывающем все ее составляющие: от физической охраны серверной до обучения персонала. Угрозы в КС многообразны и классифицируются по разным признакам (источнику, цели, способу реализации). Наибольшую опасность представляют преднамеренные искусственные угрозы (атаки), которые эксплуатируют уязвимости системы для нарушения конфиденциальности, целостности и доступности информации. Понимание этой классификации является основой для построения эффективной системы защиты.

ЭВОЛЮЦИЯ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ. ОБЩАЯ ХАРАКТЕРИСТИКА СРЕДСТВ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Часть 1: Эволюция концепции информационной безопасности (ИБ)

Введение:

Концепция ИБ не была статичной. Она развивалась параллельно с эволюцией вычислительной техники и сетей, отвечая на новые технологические вызовы и угрозы. Понимание этой эволюции позволяет осознать, почему современные системы защиты так сложны и многогранны.

Можно выделить четыре основных этапа:

Этап 1: «Компьютерная безопасность» (1960-1970-е гг.)

− Технологический контекст: Эпоха больших, дорогих мэйнфреймов – централизованных вычислительных машин, занимающих целые залы. Доступ к ним имел ограниченный круг специалистов (ученые, военные). Сетей в современном понимании не было.

− Ключевые угрозы:

1.**Физическое уничтожение или кража оборудования.**

2.**Сбои оборудования и ошибки программного обеспечения.**

3.**Несанкционированный физический доступ к терминалам** (шпионаж, саботаж).

− Парадигма защиты: «Защита периметра» в физическом смысле. Главная задача – обеспечить физическую безопасность и надежную работу самой машины.

− Основные инструменты: Замки на дверях, охрана, системы пожаротушения, резервное копирование на магнитные ленты.

Этап 2: «Безопасность данных» (1980-е гг.)

−Технологический контекст: Появление персональных компьютеров (ПК) и локальных вычислительных сетей (ЛВС). Компьютеры стали массовым инструментом, информация начала храниться децентрализованно.

− Ключевые угрозы:

1.**Компьютерные вирусы**, распространявшиеся через дискеты.

2.**Несанкционированное копирование данных** и программного обеспечения.

3.**Ошибки пользователей** на местах.

−Парадигма защиты: Защита смещается с физической машины на данные, хранящиеся на ней. Появляется необходимость контролировать доступ к файлам и бороться с вредоносным кодом.

−Основные инструменты: Антивирусное ПО, системы разграничения доступа в операционных системах (например, пароли на вход в систему), простые механизмы шифрования файлов.

Этап 3: «Сетевая / Информационная безопасность» (1990-е - 2000-е гг.)

− Технологический контекст: Взрывной рост глобальной сети Интернет. Бизнес и госучреждения массово подключаются к сети.

− Ключевые угрозы:

1.**Внешние сетевые атаки** (хакеры со всего мира).

2.**Сетевые черви и вирусы**, распространяющиеся через интернет (например, Code Red, ILOVEYOU).

3.**DoS-атаки**, фишинг, спам.

−Парадигма защиты: «Защита сетевого периметра» и данных, передаваемых по сети. Формируется классическая триада ИБ (Конфиденциальность, Целостность, Доступность). Понятие "Компьютерная безопасность" окончательно сменяется на «Информационная безопасность».

− Основные инструменты: Межсетевые экраны (Firewalls), системы обнаружения вторжений (IDS), VPN для защиты каналов связи, криптографические протоколы (SSL/TLS).

Этап 4: «Кибербезопасность и управление рисками» (2010-е гг. - настоящее время)

−Технологический контекст: Облачные вычисления, мобильные устройства, Интернет вещей (IoT), социальные сети. Понятие «периметра» размывается – данные находятся повсюду.

− Ключевые угрозы:

1.**Целенаправленные атаки (APT – Advanced Persistent Threat**), часто спонсируемые государствами.

2.**Атаки на цепочки поставок** (supply chain attacks).

3.**Программы-вымогатели** (Ransomware).

4.**Атаки с использованием социальной инженерии** на сотрудников.

−Парадигма защиты: «Нулевое доверие» (Zero Trust) – мы не доверяем никому по умолчанию, даже внутри сети. Акцент смещается с предотвращения атак (которое уже не может быть стопроцентным) на быстрое обнаружение,

реагирование и восстановление. Безопасность рассматривается как непрерывный процесс управления рисками.

− Основные инструменты: SIEM-системы (сбор и анализ событий безопасности), EDR/XDR (защита конечных точек), Threat Intelligence (анализ данных об угрозах), Security Operation Centers (SOC), регулярные пентесты (тесты на проникновение).

Часть 2: Общая характеристика средств и методов защиты информации

Для противодействия угрозам используется комплексный, эшелонированный (многоуровневый) подход, включающий различные по своей природе методы и средства защиты. Ни один из них в отдельности не может обеспечить полную безопасность.

Классификация методов и средств защиты:

1. Правовые (Законодательные) методы

Суть: Установление правил поведения и ответственности в информационной сфере на уровне государства. Создают правовое поле, в котором работают все остальные методы.

Примеры:

− Законы (в РБ: «О защите персональных данных», «Об информации, информатизации и защите информации»).

− Государственные стандарты (ГОСТ, СТБ) в области ИБ.

−Указы, постановления, регулирующие отдельные аспекты (например, Указ №40 о кибербезопасности).

−Статьи Уголовного кодекса, предусматривающие наказание за киберпреступления.

Роль: Сдерживающий фактор, определение легальных и нелегальных действий.

2. Организационные (Административные) методы

Суть: Регламентация деятельности персонала и процессов в организации для минимизации рисков ИБ. Это "бумажная" безопасность, которая управляет людьми и технологиями.

Примеры:

−Политика информационной безопасности – главный документ, определяющий цели и задачи ИБ в компании.

−Классификация информации по уровням конфиденциальности.

− Управление доступом: разработка правил, кому и к каким ресурсам предоставляется доступ.

−Обучение персонала правилам цифровой гигиены.

−План реагирования на инциденты и восстановления после сбоев.

− Физическая охрана помещений, пропускной режим.

− Роль: Фундамент системы защиты, управление самым слабым звеном – человеком.

3. Программно-технические методы

Суть: Использование специализированного аппаратного и программного обеспечения для непосредственной защиты компонентов компьютерной системы.

Примеры (основные категории):

− Идентификация и аутентификация: Проверка того, что пользователь является тем, за кого себя выдает (пароли, биометрия, токены, 2FA/MFA).

−Управление доступом: Механизмы, реализующие организационные правила (например, списки контроля доступа ACL).

− Криптографические средства: Шифрование данных при хранении и передаче, использование электронной цифровой подписи (ЭЦП).

− Защита от вредоносного ПО: Антивирусы, песочницы (sandboxes).

−Сетевая защита: Межсетевые экраны (Firewalls), системы обнаружения/предотвращения вторжений (IDS/IPS), VPN.

−Анализ и мониторинг: SIEM-системы, сканеры уязвимостей.

− Роль: «Щит и меч» информационной безопасности, техническая реализация политик.

4. Физические методы

Суть: Создание физических препятствий для предотвращения несанкционированного доступа к оборудованию и носителям информации.

Примеры:

−Надежные замки, решетки на окнах, укрепленные двери в серверных.

−Системы контроля и управления доступом (СКУД) – электронные пропуска, турникеты.

−Системы видеонаблюдения.

−Охранная и пожарная сигнализация.

− Роль: Первый, базовый уровень защиты. Без него все остальные методы могут оказаться бесполезными.

Эволюция концепции ИБ прошла путь от физической защиты компьютера к комплексному управлению рисками в киберпространстве. Современная система защиты информации – это эшелонированная оборона, которая строится на гармоничном сочетании четырех видов методов: правовых (законы), организационных (политики и люди), программно-технических (ПО и «железо») и физических (замки и охрана). Только их совместное применение позволяет эффективно противостоять современным угрозам.

ПОВЫШЕНИЕ ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Надежность компьютерной системы (КС) – это ее способность выполнять заданные функции, сохраняя свои эксплуатационные показатели в установленных пределах в течение требуемого промежутка времени. В контексте информационной безопасности, надежность является фундаментом для обеспечения доступности информации и сервисов. Если система ненадежна, она может отказать в любой момент, и легитимные пользователи потеряют доступ к данным, что является прямым нарушением принципа доступности.

1. Основные понятия и метрики

Для понимания темы необходимо четко различать следующие понятия:

− Сбой (Fault): Аппаратная или программная аномалия, первопричина проблемы. Пример: физическое повреждение сектора на жестком диске, ошибка в коде программы.

− Ошибка (Error): Некорректное состояние системы, вызванное сбоем. Система переходит в состояние, которое может привести к отказу. Пример: операционная система не может прочитать данные с поврежденного сектора.

− Отказ (Failure): Наблюдаемое извне отклонение поведения системы от спецификации. Система перестает выполнять свою функцию. Пример: приложение «зависает» или выдает критическую ошибку, веб-сайт недоступен.

Цель повышения надежности – предотвратить переход сбоя в ошибку, а ошибки – в отказ.

Ключевые метрики надежности:

− MTBF (Mean Time Between Failures) – среднее время наработки на отказ. Чем выше этот показатель, тем надежнее система.

− MTTR (Mean Time To Repair) – среднее время восстановления после отказа. Чем ниже, тем лучше.

− Доступность (Availability) – вероятность того, что система будет работоспособна в произвольный момент времени. Рассчитывается как:

Availability = MTBF / (MTBF + MTTR)

Доступность часто измеряется в «девятках»:

Уровень доступности	**% времени работы**	**Допустимое время простоя в год**
99% («две девятки»)	99.0%	~3.65 дня
99.9% («три девятки»)	99.9%	~8.76 часа
99.99% («четыре девятки»)	99.99%	~52 минуты
99.999% («пять девяток»)	99.999%	~5 минут

2. Фундаментальный принцип: Отсутствие единой точки отказа (No Single Point of Failure - SPOF)

Единая точка отказа (SPOF) – это компонент системы, отказ которого приводит к отказу всей системы.

Основная стратегия повышения надежности заключается в проектировании архитектуры, в которой нет единых точек отказа. Это достигается за счет резервирования (Redundancy).

3. Практические методы и технологии повышения надежности

Методы можно сгруппировать по уровням системы, на которые они направлены.

3.1. Аппаратное резервирование

Резервирование электропитания:

− Источники бесперебойного питания (ИБП / UPS): Обеспечивают кратковременную работу при отключении основного питания, позволяя корректно завершить работу или дождаться запуска генератора.

− Несколько блоков питания (Redundant Power Supplies): В серверах устанавливаются два или более блока питания, подключенных к разным источникам. При отказе одного, второй мгновенно берет на себя всю нагрузку.

Резервирование систем хранения данных:

− RAID (Redundant Array of Independent Disks): Технология объединения нескольких дисков в один логический массив для повышения производительности и/или надежности.

−RAID 1 (Зеркалирование): Данные полностью дублируются на два диска. При отказе одного диска система продолжает работать со вторым. Высокая надежность, но теряется 50% емкости.

− RAID 5 (Чередование с четностью): Данные и контрольные суммы (четность) распределяются по всем дискам. Выдерживает отказ одного диска. Экономичнее, чем RAID 1.

− RAID 10 (1+0): Комбинация зеркалирования и чередования. Высокая производительность и надежность. Выдерживает отказ одного диска в каждой зеркальной паре.

Резервирование сетевых подключений:

− **Несколько сетевых карт** (NIC Teaming / Bonding): Объединение двух и более сетевых адаптеров в один логический. Если один кабель или адаптер выходит из строя, трафик идет через оставшиеся.

3.2. Программное и системное резервирование

Кластеризация (Clustering) – объединение нескольких серверов (узлов) в единую систему, которая выглядит для пользователя как один сервер.

Отказоустойчивый кластер (Failover Cluster):

− Active/Passive: Один узел (активный) обрабатывает запросы, второй (пассивный) находится в режиме ожидания. При отказе активного узла пассивный мгновенно перехватывает его роль.

−Active/Active: Все узлы кластера одновременно обрабатывают нагрузку. При отказе одного узла его нагрузка перераспределяется между оставшимися.

Балансировка нагрузки (Load Balancing) – распределение входящих запросов между несколькими серверами. Балансировщик проверяет доступность серверов и не отправляет трафик на отказавший узел, тем самым повышая общую доступность сервиса.

Виртуализация. Современные технологии виртуализации (VMware, Hyper-V) предоставляют мощные инструменты для повышения надежности:

− Live Migration (vMotion): Перемещение работающей виртуальной машины с одного физического сервера на другой без остановки ее работы (например, для проведения технического обслуживания хоста).

−High Availability (HA): Автоматический перезапуск виртуальной машины на другом сервере кластера в случае отказа ее текущего хоста.

3.3. Резервирование данных и планов восстановления

Резервное копирование (Backup) – процесс создания копий данных для их последующего восстановления в случае утери или повреждения. **Это последний рубеж обороны.**

Правило «3-2-1»: иметь 3 копии данных, на 2 разных типах носителей, 1 из которых хранится за пределами основной площадки (off-site).

RPO (Recovery Point Objective): максимально допустимый период, за который могут быть потеряны данные. Определяет, как часто нужно делать бэкапы.

RTO (Recovery Time Objective): максимально допустимое время восстановления системы после сбоя.

Репликация данных: непрерывное копирование данных на резервный сервер или СХД. В отличие от бэкапа, реплика почти всегда актуальна.

3.4. Процессные (организационные) методы

Мониторинг и оповещение: автоматизированные системы (Zabbix, Prometheus) постоянно отслеживают состояние ключевых компонентов (CPU, RAM, диски, сетевая доступность) и отправляют оповещения администраторам при отклонении от нормы, позволяя реагировать на проблемы до того, как они приведут к отказу.

Регулярное техническое обслуживание: своевременное обновление ПО, установка патчей безопасности, проверка состояния оборудования.

План аварийного восстановления (Disaster Recovery Plan - DRP): четко прописанный алгоритм действий для всех сотрудников в случае серьезного сбоя или катастрофы.

Важнейший элемент DRP – его регулярное тестирование.

Повышение эксплуатационной надежности – это **комплексный, многоуровневый процесс**, направленный на обеспечение доступности информации. Его основой является архитектурный принцип **«отсутствия единой точки отказа» (SPOF)**, который реализуется через **резервирование** на всех уровнях: аппаратном (ИБП, RAID), системном (кластеризация, балансировка), уровне данных (бэкапы) и организационном (мониторинг, DRP). Надежная система – это не та, что никогда не ломается, а та, чей отказ компонента не приводит к отказу всей системы и которая может быть быстро восстановлена.

ОБЩАЯ ХАРАКТЕРИСТИКА ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Если программно-технические средства – это «замки и стены» в системе защиты информации, то организационное обеспечение – это «**законы, правила и служба безопасности»**, которые определяют, кто, как и когда может пользоваться этими замками и ходить внутри стен.

Определение: Организационное обеспечение защиты информации – это комплекс административных, процедурных и режимных мер, направленных на формирование и поддержание безопасной информационной среды в организации путем управления персоналом, процессами и физическим доступом.

Ключевая идея: Технологии лишь реализуют те правила, которые устанавливаются на организационном уровне. Организационные меры **первичны,** а технические – **вторичны**.

Часть 1: Общая характеристика организационного обеспечения

Цель организационных мер – минимизировать риски, связанные с **человеческим фактором** (как умышленные, так и неумышленные действия) и создать контролируемую среду функционирования информационных систем.

Основные направления организационного обеспечения:

1. Управление персоналом (Работа с кадрами)

Это непрерывный процесс на протяжении всего жизненного цикла сотрудника в компании.

Прием на работу:

− Проверка кандидатов (background check) на должности, связанные с доступом к критичной информации.

− Подписание соглашения о неразглашении (NDA – Non-Disclosure Agreement) и обязательства о соблюдении коммерческой тайны.

Обучение и повышение осведомленности:

−Первичный инструктаж по ИБ для всех новых сотрудников.

− Регулярные тренинги по актуальным угрозам (например, как распознать фишинг).

−Тестирование знаний персонала.

Текущая работа:

− Четкое определение должностных обязанностей и зон ответственности.

− Мотивация сотрудников к соблюдению правил ИБ.

Увольнение или перевод на другую должность:

− Разработанная процедура прекращения доступа (немедленное блокирование учетных записей, изъятие пропусков, ключей).

− Контроль за возвратом всех материальных активов.

Физическая защита

Обеспечение безопасности физического периметра организации и ключевых помещений.

Контроль физического доступа:

− Пропускной режим (охрана, турникеты).

− Системы контроля и управления доступом (СКУД) на основе электронных карт.

− Замки на дверях серверных, архивов.

Защита оборудования:

− Правила «чистого стола и чистого экрана» (не оставлять документы и разблокированный компьютер без присмотра).

− Опечатывание системных блоков, портов.

Обеспечение среды функционирования:

Системы бесперебойного питания, кондиционирования, пожаротушения в серверных.

3. Документационное обеспечение (Политики и процедуры)

Создание системы внутренних нормативных документов, которые формализуют все требования ИБ. Это «бумажная безопасность», которая является основой для всех действий.

Иерархия документов:

1. Политика (Концепция) информационной безопасности: Верхнеуровневый документ, декларирующий цели, задачи и принципы обеспечения ИБ в организации. Утверждается высшим руководством.

2. Частные политики и положения: Документы, детализирующие отдельные направления (Политика управления доступом, Положение о коммерческой тайне).

3. Регламенты и процедуры: Пошаговые инструкции для выполнения конкретных задач (Регламент резервного копирования, Процедура реагирования на инциденты).

4. Должностные инструкции: Закрепление ответственности за ИБ за конкретными сотрудниками.

5. Управление доступом

Организационное определение правил предоставления доступа к информационным ресурсам.

Принцип минимальных привилегий (Least Privilege): Пользователю предоставляется только тот минимальный набор прав, который необходим ему для выполнения его должностных обязанностей.

Принцип «необходимо знать» (Need-to-Know): Доступ к конкретной информации предоставляется только тем, кому она нужна для работы.

Матрица доступа: Таблица, в которой четко прописано, какой субъект (пользователь, группа) какой тип доступа (чтение, запись, выполнение) имеет к какому объекту (файл, папка, система).

6. Управление инцидентами и непрерывностью бизнеса

План реагирования на инциденты (Incident Response Plan): Алгоритм действий при обнаружении инцидента ИБ (кто, кому и что сообщает; как локализовать угрозу; как восстановить систему).

План аварийного восстановления (Disaster Recovery Plan - DRP): Технический план по восстановлению IT-инфраструктуры после серьезной аварии или катастрофы.

План обеспечения непрерывности бизнеса (Business Continuity Plan - BCP): Более широкий план, который описывает, как организация будет продолжать выполнять свои критически важные функции во время и после чрезвычайной ситуации.

Часть 2: Организационно-правовое обеспечение

Определение: Организационно-правовое обеспечение – это совокупность организационных мер, которые реализуются на основе и во исполнение требований законодательства в области защиты информации.

Это связующее звено между государственным регулированием и практической деятельностью компании. Закон говорит, что нужно защищать и устанавливает ОТВЕТСТВЕННОСТЬ, а организационные меры компании определяют КАК это будет сделано.

Иерархия правового регулирования:

1. Уровень 1: Законодательные акты (Законы)

Устанавливают фундаментальные принципы, права, обязанности и ответственность.

Примеры в РБ:

Конституция РБ: Закрепляет базовые права на защиту информации о частной жизни и персональных данных.

Закон № 99-З «О защите персональных данных»: Требует от организаций (операторов) принимать правовые, организационные и технические меры для защиты ПДн.

Закон «Об информации, информатизации и защите информации»: Определяет общие подходы к защите информации, вводит понятия собственника информации, конфиденциальности и т.д.

Трудовой кодекс: Позволяет устанавливать материальную ответственность за разглашение коммерческой тайны.

Уголовный кодекс: Устанавливает уголовную ответственность за компьютерные преступления.

2. Уровень 2: Подзаконные акты и стандарты

Конкретизируют и детализируют требования законов.

Примеры в РБ:

Указы Президента РБ (например, №40 о кибербезопасности, №60 о регулировании национального сегмента сети Интернет).

Постановления Совета Министров, приказы ОАЦ.

Государственные стандарты (СТБ): Содержат детальные требования к системам защиты информации, процессам аудита и т.д. Их применение может быть обязательным для госорганов и критически важных объектов.

3. Уровень 3: Локальные нормативные правовые акты (ЛНПА) организации

Это **внутренние документы компании**, которые реализуют требования вышестоящих уровней. Именно они и составляют основу организационного обеспечения.

Примеры:

Положение о коммерческой тайне.

Политика обработки персональных данных.

Приказы о назначении ответственных за ИБ.

Все политики, регламенты и инструкции, перечисленные в Части 1.

Схема взаимодействия:

Закон (например, «О защите ПДн») → Требование (организация обязана защищать ПДн) → Организационная мера (разработка «Положения об обработке и защите ПДн», назначение ответственного, обучение персонала) → Техническая мера (внедрение шифрования, антивируса).

Организационное обеспечение является фундаментом системы информационной безопасности. Оно управляет самым непредсказуемым элементом – человеком – и определяет «правила игры» для технологий. Организационно-правовое обеспечение представляет собой практическую реализацию требований законодательства через систему внутренних политик,

регламентов и процедур. Без проработанных организационных мер любые, даже самые дорогие технические средства, будут неэффективны.

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ (КСЗИ). КОНЦЕПЦИЯ КСЗИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ. ФУНКЦИОНИРОВАНИЯ КСЗИ

В реальном мире применение разрозненных, не связанных между собой инструментов неэффективно. Злоумышленник всегда будет искать самую слабую, незащищенную лазейку.

Ответом на этот вызов стал переход от «лоскутной» защиты к построению **Комплексной системы защиты информации (КСЗИ).**

Аналогия: Оборона крепости. Нельзя просто построить высокую стену (Firewall), забыв про ворота (слабые пароли), подкопы (инсайдеры) и стражу на стенах (мониторинг). Эффективна только система, где все элементы защиты взаимосвязаны и дополняют друг друга.

Определение: КСЗИ – это упорядоченная совокупность взаимосвязанных правовых, организационных, инженерно-технических и программно-аппаратных средств и методов, направленная на противодействие всему спектру актуальных угроз и обеспечение заданного уровня защищенности информации в компьютерной системе.

Часть 1: Концепция КСЗИ (Принципы построения)

Концепция КСЗИ базируется на нескольких фундаментальных принципах, которые и делают ее комплексной и системной.

1. Принцип системности (Systemic Approach)

Суть: Защита информации рассматривается не как набор отдельных мер, а как единая целостная система. Все компоненты защиты (люди, процессы, технологии) взаимосвязаны. Безопасность закладывается на этапе проектирования информационной системы, а не «прикручивается» сверху после ее создания.

На практике: Изменение одного элемента (например, ввод нового ПО) требует анализа его влияния на всю систему безопасности.

2. Принцип эшелонированной обороны (Defense in Depth)

Суть: Создание нескольких рубежей (эшелонов) защиты на пути злоумышленника. Если он преодолеет один рубеж, его должен остановить следующий. Это исключает наличие единой точки отказа.

Пример эшелонов от внешнего к внутреннему:

1. **Физический уровень:** Охрана здания, СКУД в серверную.
2. **Сетевой периметр:** Межсетевой экран (Firewall) на границе сети.
3. **Уровень сети:** Сегментация сети (VLAN), системы обнаружения вторжений (IDS/IPS).

4. **Уровень хоста (ОС):** Настроенный брандмауэр ОС, антивирус, регулярные обновления.

5. **Уровень приложений:** Защита от веб-атак (WAF), безопасная разработка ПО.

6. **Уровень данных:** Шифрование баз данных, разграничение доступа к файлам.

7. **Организационный уровень (охватывает все):** Обучение пользователей, политики безопасности.

3. Принцип непрерывности (Continuity)

Суть: Защита информации – это непрерывный процесс, а не разовый проект. Угрозы постоянно эволюционируют, поэтому система защиты должна постоянно анализироваться, обновляться и совершенствоваться.

На практике: Реализуется через цикл PDCA (Plan-Do-Check-Act):

−Plan (Планируй): Анализ рисков, разработка политик.

− Do (Делай): Внедрение средств защиты, обучение персонала.

− Check (Проверяй): Мониторинг, аудит, тесты на проникновение (пентесты).

− Act (Действуй): Устранение недостатков, совершенствование системы.

4. Принцип централизованного управления и мониторинга (Centralized Management)

Суть: Все подсистемы защиты должны управляться и контролироваться из единого центра. Это позволяет видеть целостную картину происходящего, оперативно выявлять сложные атаки и координировать ответные действия.

На практике: Создание **Центра управления безопасностью (Security Operation Center - SOC),** использование SIEM-систем для сбора и корреляции событий со всех источников (Firewall, антивирусы, серверы).

5. Принцип экономической целесообразности (Cost-Effectiveness)

Суть: Стоимость внедрения и эксплуатации КСЗИ не должна превышать размер потенциального ущерба от реализации угроз. Защита должна быть адекватной ценности защищаемых активов.

На практике: Проводится анализ рисков (Risk Assessment), который помогает определить, какие активы и от каких угроз нужно защищать в первую очередь, и сколько на это целесообразно потратить.

Часть 2: Функционирование КСЗИ (Подсистемы и их взаимодействие)

Функционирование КСЗИ можно представить как работу нескольких взаимосвязанных подсистем, реализующих полный цикл управления безопасностью.

Подсистема	Задача	Ключевые технологии и методы
1. Подсистема предотвращения (Prevention)	Проактивно блокировать известные угрозы и не допускать нарушений.	**Управление доступом:** аутентификация (пароли, 2FA), авторизация. **Сетевая защита:** Firewalls, VPN, прокси-серверы. **Защита от вредоносного ПО:** Антивирусы, песочницы. **Физическая защита:** СКУД, видеонаблюдение.
2. Подсистема обнаружения (Detection)	Выявлять инциденты, которые не удалось предотвратить.	**Мониторинг и анализ:** SIEM-системы, системы обнаружения вторжений (IDS/IPS). **Аудит и логирование:** Сбор и анализ журналов событий с серверов и оборудования. **Анализ уязвимостей:** Сканеры уязвимостей (Nessus, MaxPatrol).
3. Подсистема реагирования (Response)	Оперативно локализовать инцидент и минимизировать ущерб.	**План реагирования на инциденты (IRP):** Четкий алгоритм действий. **Средства изоляции:** Блокировка IP-адресов на Firewall, отключение зараженного хоста от сети. **Сбор доказательств:** Инструменты цифровой криминалистики (форензики).
4. Подсистема восстановления (Recovery)	Вернуть систему в штатное рабочее состояние после инцидента.	**Резервное копирование и восстановление:** Системы бэкапов. **План аварийного восстановления (DRP):** Процедуры восстановления IT-инфраструктуры. **Анализ инцидента:** "Работа над ошибками" для предотвращения повторения.
5. Подсистема управления (Management)	Координировать работу всех подсистем, обеспечивать их актуальность.	**Политики и процедуры:** Разработка и обновление документации. **Управление рисками:** Регулярная оценка и обработка рисков. **Обучение персонала:** Повышение осведомленности.

Цикл функционирования: Система постоянно находится в режиме предотвращения. Средства **обнаружения** непрерывно сканируют систему на предмет аномалий. При фиксации инцидента активируется подсистема реагирования. После локализации угрозы подсистема восстановления возвращает систему в рабочее состояние. Весь этот процесс координируется подсистемой

управления, которая анализирует инцидент и вносит изменения в работу других подсистем для улучшения защиты.

КСЗИ – это не продукт, который можно купить и установить, а **непрерывный процесс и система**, построенная на принципах эшелонированной обороны, непрерывности, централизованного управления и экономической целесообразности. Ее функционирование представляет собой замкнутый цикл: **Предотвращение → Обнаружение → Реагирование → Восстановление,** который координируется единой подсистемой управления. Эффективность КСЗИ определяется не столько мощностью отдельных компонентов, сколько их **грамотной интеграцией и взаимодействием.**

II. ПРАКТИЧЕСКИЙ РАЗДЕЛ

ПЛАНЫ И ЗАДАНИЯ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1
Разработка памятки для граждан по защите персональных данных в интернете

Тема: Защита персональных данных в сети Интернет.

Цель работы:

Систематизировать знания об основных угрозах безопасности персональных данных, с которыми сталкиваются рядовые пользователи.

Овладеть практическими навыками разработки информационных материалов (памяток, инструкций), направленных на повышение цифровой грамотности населения.

Научиться адаптировать сложную информацию для конкретной целевой аудитории, используя ясный, доступный и убедительный язык.

1. Теоретическая часть

Ежедневно миллионы граждан используют интернет для общения, работы, покупок и получения услуг, оставляя после себя цифровой след – свои персональные данные (ПДн). К ним относятся не только ФИО и паспортные данные, но и номера телефонов, адреса, e-mail, IP-адреса, геолокация, фотографии и даже поведенческая информация (что мы ищем, что покупаем).

Эти данные являются ценным товаром для мошенников, спамеров и других злоумышленников. Основные угрозы, с которыми сталкиваются граждане:

–Фишинг: Массовая рассылка поддельных писем (от имени банков, соцсетей, госорганов) с целью кражи логинов, паролей и данных банковских карт.

–Социальная инженерия: Психологическая манипуляция, чаще всего через телефонные звонки или мессенджеры (звонки «из банка», «из милиции»), с целью заставить человека добровольно сообщить свои данные или перевести деньги.

– Вредоносное ПО (Malware): Установка на компьютер или смартфон программ-шпионов, которые крадут пароли, данные карт и другую информацию.

– Публичные сети Wi-Fi: Перехват незашифрованных данных при подключении к небезопасным сетям в кафе, аэропортах и т.д.

– Чрезмерная откровенность (Oversharing): Публикация в открытом доступе (в соцсетях) слишком большого количества личной информации, которую могут использовать злоумышленники.

Задача данной работы – создать памятку, которая в простой и понятной форме объяснит пользователям, как защититься от этих угроз.

2. Порядок выполнения работы

1). Выберите вариант индивидуального задания, определив свою целевую аудиторию.

2). Продумайте структуру памятки. Она должна быть логичной и легко читаемой. Рекомендуемая структура:

−Название: Яркое и привлекающее внимание (например, «Ваши данные под защитой: 5 правил безопасности в интернете»).

− Введение: Краткое объяснение, почему защита данных важна.

− Основные угрозы: 3-4 главные опасности, описанные простым языком.

− Золотые правила защиты: 5-7 ключевых, практических советов (что конкретно делать).

−Что делать, если...: Краткая инструкция на случай, если данные все-таки утекли или вас обманули.

3). Напишите текст памятки, адаптируя язык, тон и примеры под вашу целевую аудиторию. Избегайте сложной технической терминологии!

4). Продумайте визуальное оформление: используйте списки, пиктограммы (иконки), выделение ключевых моментов жирным шрифтом или цветом, чтобы сделать памятку наглядной и легко воспринимаемой.

5). Напишите краткую пояснительную записку (1-2 абзаца), в которой обоснуйте, почему вы выбрали именно такую структуру, тон и акценты для вашей целевой аудитории.

6). Оформите результаты в виде готовой памятки (1-2 страницы) и пояснительной записки.

3. Индивидуальные задания

Вариант 1. Целевая аудитория: Подростки и студенты (14-18 лет)

Активные пользователи социальных сетей, онлайн-игр и мессенджеров. Технически грамотны, но часто пренебрегают приватностью.

Акценты в памятке: Безопасность в соцсетях, защита игровых аккаунтов, кибербуллинг, риски публикации личных фото.

Тон: Современный, динамичный, можно использовать понятный им сленг.

Вариант 2. Целевая аудитория: Взрослые работающие люди (30-50 лет)

Активно пользуются интернет-банкингом, онлайн-магазинами, госуслугами. Главная цель – защита финансов и данных своей семьи.

Акценты в памятке: Финансовая безопасность, защита от фишинга, безопасные онлайн-покупки, защита детских аккаунтов.

Тон: Деловой, прагматичный, вызывающий доверие.

Вариант 3. Целевая аудитория: Пожилые люди (65+ лет)

Часто менее уверены в своих технических навыках, доверчивы, являются основной мишенью для телефонной и интернет-социальной инженерии.

Акценты в памятке: Распознавание мошеннических звонков и сообщений в мессенджерах, базовые правила безопасности (не сообщать код из SMS), общение с «родственниками» в соцсетях.

Тон: Максимально простой, уважительный, спокойный. Шрифт должен быть крупным.

Практическое занятие 2
Анализ уязвимостей компьютерной системы с использованием сканера безопасности

Тема: Анализ и управление уязвимостями.

Цель работы:

Освоить базовые принципы работы автоматизированных сканеров безопасности.

Овладеть практическими навыками запуска сканирования, интерпретации отчетов и приоритизации найденных уязвимостей.

Научиться формировать рекомендации по устранению критических уязвимостей на основе данных сканера.

1. Теоретическая часть

Уязвимость – это недостаток в программном или аппаратном обеспечении, который может быть использован злоумышленником для нарушения безопасности системы. Ручной поиск уязвимостей – трудоемкий процесс, поэтому для автоматизации используются сканеры безопасности.

Сканер безопасности– это программа, которая автоматически проверяет целевую систему (сеть, сервер, веб-приложение) на наличие известных уязвимостей.

–Как он работает? Сканер отправляет на цель специально сформированные запросы и анализирует ответы. Сравнивая их с базой данных известных атак и уязвимостей (сигнатур), он делает вывод о наличии проблемы.

–Классификация уязвимостей: Для оценки серьезности уязвимостей часто используется система CVSS (Common Vulnerability Scoring System), которая присваивает рейтинг от 0 до 10. Уязвимости принято делить на уровни риска: Low (Низкий), Medium (Средний), High (Высокий), Critical (Критический).

– OWASP Top 10: Это всемирно признанный рейтинг самых критических рисков безопасности веб-приложений. Сканеры часто ориентируются на поиск именно этих уязвимостей (например, SQL Injection, Cross-Site Scripting (XSS), Security Misconfiguration).

В данной работе мы будем использовать OWASP ZAP (Zed Attack Proxy) – бесплатный, популярный сканер с открытым исходным кодом, предназначенный для поиска уязвимостей в веб-приложениях. В качестве цели будет выступать специально созданное уязвимое приложение OWASP Juice Shop, что позволяет проводить сканирование легально и безопасно.

2. Порядок выполнения работы

1). Подготовка рабочего места:

– Запустить сканер безопасности OWASP ZAP.

− Запустить целевое веб-приложение OWASP Juice Shop (например, через Docker или по ссылке, предоставленной преподавателем). Убедиться, что приложение доступно в браузере.

2). Проведение автоматического сканирования:

− В стартовом окне OWASP ZAP выбрать «Automated Scan».

−В поле «URL to attack» ввести адрес запущенного приложения (например, http://localhost:3000).

− Нажать кнопку «Attack». Дождаться завершения сканирования (процесс может занять 10-20 минут).

3). Анализ результатов:

− После завершения сканирования перейти на вкладку «Alerts» (Оповещения) в левой нижней части экрана.

− Изучить список найденных уязвимостей. Обратить внимание на их название, уровень риска (флажок: красный – высокий, оранжевый – средний) и количество найденных экземпляров.

4). Формирование отчета:

−Создать сводную таблицу найденных уязвимостей с уровнем риска Medium и выше. Таблица должна содержать столбцы: «Название уязвимости», «Уровень риска», «Количество».

−Выбрать одну уязвимость с уровнем риска High (или Medium, если High не найдены), соответствующую вашему варианту.

− Подробно описать эту уязвимость:

−В чем ее суть? (Используя описание из ZAP во вкладке справа).

− Какой ущерб она может нанести? (Нарушение конфиденциальности, целостности, доступности).

−Привести конкретный пример URL, где она была найдена.

− Предложить рекомендации по устранению, основываясь на разделе «Solution» в описании уязвимости в ZAP.

5). Оформить результаты в виде структурированного отчета.

3. Индивидуальные задания

Для детального анализа выберите одну уязвимость высокого/среднего риска из категории, соответствующей вашему варианту:

Вариант 1: Уязвимости, связанные с инъекциями (Injection). Например, SQL Injection, Cross-Site Scripting (XSS).

Вариант 2: Уязвимости, связанные с небезопасной конфигурацией. Например, Directory Browsing, Private IP Disclosure, Password Autocomplete in browser.

Вариант 3: Уязвимости, связанные с раскрытием чувствительной информации. Например, Information Disclosure, Source Code Disclosure.

Практическое занятие 3
Сравнительный анализ средств защиты информации различных поколений

Тема: Сравнительный анализ средств защиты информации различных поколений.

Цель работы:

Систематизировать знания о различных классах и типах средств защиты информации (СЗИ).

Научиться классифицировать СЗИ в соответствии с историческими этапами (поколениями) эволюции концепции ИБ.

Овладеть практическими навыками подбора адекватного и комплексного набора СЗИ для защиты современной IT-инфраструктуры, обосновывая необходимость применения инструментов каждого поколения.

1. Теоретическая часть

Эволюция угроз информационной безопасности привела к появлению нескольких поколений средств защиты. Важно понимать, что каждое новое поколение не заменяло предыдущее, а дополняло его, создавая многоуровневую, эшелонированную оборону.

Условная классификация поколений СЗИ:

1). Поколение 1: Физическая безопасность (1960-70-е)

Задачи: Защита больших мэйнфреймов от физического доступа и сбоев.

Средства: Замки, охрана, системы пожаротушения, резервное копирование на ленты.

2). Поколение 2: Безопасность конечных точек (хостов) (1980-е)

Задачи: Защита персональных компьютеров от вирусов и несанкционированного доступа.

Средства: Антивирусное ПО, системы разграничения доступа в ОС (пароли, ACL).

3). Поколение 3: Безопасность сетевого периметра (1990-2000-е)

Задачи: Защита локальной сети от угроз из глобальной сети Интернет.

Средства: Межсетевые экраны (Firewall), системы обнаружения/предотвращения вторжений (IDS/IPS), VPN-шлюзы.

4). Поколение 4: Безопасность данных и приложений (2010-е - н.в.)

Задачи: Защита от сложных, целенаправленных атак (APT) в условиях «размытого» периметра (облака, мобильные устройства). Обнаружение угроз на основе анализа поведения и данных.

Средства: SIEM-системы (анализ событий), EDR (продвинутая защита хостов), WAF (защита веб-приложений), DLP (предотвращение утечек), Threat Intelligence (анализ угроз).

Современная эффективная система защиты обязательно включает в себя инструменты всех поколений.

2. Порядок выполнения работы

1). Выберите вариант индивидуального задания.

2). Проанализируйте IT-инфраструктуру и ключевые риски описанной организации.

3). Разработайте комплексную систему защиты, подобрав не менее 6-8 средств защиты информации из разных поколений (2, 3 и 4).

4). Заполните аналитическую таблицу «Эшелонированная система защиты», в которой для каждого выбранного СЗИ необходимо:

Указать его поколение.

Дать краткую характеристику.

Обосновать необходимость его применения в данной инфраструктуре, ответив на вопрос: «Какую проблему оно решает и почему средства предыдущих поколений с этой задачей не справляются?»

5). Сформулируйте вывод о том, почему защита, построенная только на инструментах одного поколения (например, только антивирус и Firewall), будет неэффективна в современных условиях.

3. Индивидуальные задания

Вариант 1. Организация: Современный завод

Завод с двумя основными сетями: корпоративной (офисной) сетью, где работают бухгалтерия и менеджмент, и технологической сетью (АСУ ТП), которая управляет станками и конвейером. Ранее сети были изолированы, но сейчас для мониторинга и сбора данных их объединили через специальный шлюз.

Вариант 2. Организация: Облачный IT-стартап

Компания разрабатывает SaaS-продукт. Вся инфраструктура (серверы, базы данных, хранилища) находится в публичном облаке (например, AWS или Yandex.Cloud). Физических серверов у компании нет. Сотрудники работают удаленно из разных точек мира.

Вариант 3. Организация: Коммерческий банк

Банк с большой филиальной сетью. Имеет собственный дата-центр, корпоративную сеть, публичный веб-сайт и систему интернет-банкинга. Является объектом критической информационной инфраструктуры и главной целью для финансовых киберпреступников.

Практическое занятие 4
Разработка политики информационной безопасности для организаций

Тема: Разработка Политики информационной безопасности для организации.

Цель работы:

Изучить структуру и назначение Политики информационной безопасности как основополагающего организационно-распорядительного документа.

Овладеть практическими навыками формулирования целей, задач и основных положений Политики ИБ.

Научиться адаптировать содержание Политики под специфику деятельности, культуру и ключевые риски конкретной организации.

1. Теоретическая часть

Политика информационной безопасности (Information Security Policy) – это официальный, верхнеуровневый документ, утвержденный руководством, который декларирует цели, принципы и подходы организации к защите информации.

Ключевые характеристики Политики:

Это не техническая инструкция. Она не описывает, как настраивать Firewall или какой антивирус использовать.

Это документ для всех сотрудников. Она написана понятным языком и определяет общие правила игры и меру ответственности каждого.

Это фундамент. На ее основе разрабатываются все остальные, более детальные документы: положения, регламенты, инструкции.

Она демонстрирует позицию руководства. Принятие Политики – это заявление о том, что руководство осознает важность ИБ и готово выделять на нее ресурсы.

Типовая структура Политики информационной безопасности:

1). Общие положения: Назначение документа, введение в действие, сроки пересмотра.

2). Цели и задачи: Что мы хотим достичь с помощью ИБ (например, «обеспечить непрерывность бизнеса», «защитить репутацию», «соответствовать требованиям законодательства»).

3). Область применения: На кого и на какие активы распространяется действие Политики (все сотрудники, подрядчики, все информационные системы).

4). Основные принципы ИБ: Фундаментальные правила (принцип минимальных привилегий, эшелонированная оборона, персональная ответственность).

5). Распределение ролей и ответственности: Кто за что отвечает в области ИБ (руководство, IT-отдел, служба безопасности, каждый сотрудник).

6). Ответственность за нарушения: Указание на то, что несоблюдение Политики повлечет за собой дисциплинарные взыскания в соответствии с законодательством.

7). Ссылки на связанные документы: Перечень частных политик (политика управления доступом, политика резервного копирования и т.д.), которые детализируют данный документ.

2. Порядок выполнения работы

1). Выберите вариант индивидуального задания.

2). Проанализируйте специфику организации из вашего варианта: ее основные цели, ценности, риски и корпоративную культуру.

3). Разработайте проект Политики информационной безопасности для данной организации. Документ должен иметь четкую структуру, соответствующую теоретической части.

4). Наполните каждый раздел конкретным содержанием, адаптированным под вашу организацию. Например, в разделе «Цели» для банка главной целью будет защита финансовой тайны, а для завода – обеспечение непрерывности технологического процесса.

5). Напишите краткую пояснительную записку (2-3 абзаца), в которой обоснуйте ключевые решения, принятые при разработке Политики. (Например: «Политика для креативного агентства намеренно написана в менее формальном тоне, чтобы соответствовать корпоративной культуре, однако четко определяет ответственность за данные клиентов...»).

6). Оформите результаты в виде проекта документа (2-3 страницы) и пояснительной записки к нему.

3. Индивидуальные задания

Вариант 1. Организация: Производственное предприятие (завод)

Завод, производящий уникальное оборудование. Ключевые активы: конструкторская документация (чертежи), технологические процессы (ноу-хау), система управления производством (АСУ ТП). Культура формальная, иерархическая.

Вариант 2. Организация: Креативное digital-агентство

Компания, занимающаяся рекламой, дизайном и SMM для крупных брендов. Ключевые активы: данные клиентов (маркетинговые стратегии), результаты творческой работы, репутация. Культура гибкая, неформальная, многие работают удаленно.

Вариант 3. Организация: Частный медицинский центр

Клиника, предоставляющая широкий спектр медицинских услуг. Ключевые активы: персональные данные и истории болезней пациентов (врачебная тайна, особо защищаемая информация). Деятельность строго регулируется законодательством.

Практическое занятие 5
Разработка концепции создания КСЗИ для организации

Цель работы:

Сформировать целостное представление о КСЗИ как о единой, управляемой системе.

Овладеть практическими навыками разработки стратегического документа – Концепции создания КСЗИ.

Научиться определять цели, задачи, принципы и архитектурные решения для построения системы защиты, исходя из бизнес-целей и модели угроз конкретной организации.

1. Теоретическая часть

Концепция создания КСЗИ – это основополагающий стратегический документ, который определяет видение, цели, принципы и общую архитектуру будущей системы защиты информации. В отличие от Политики ИБ, которая устанавливает «законы и правила» для всех, Концепция является "генеральным планом" для построения самой системы защиты.

Назначение Концепции:

Обосновать перед руководством необходимость создания или модернизации КСЗИ.

Определить единый вектор развития системы ИБ.

Зафиксировать ключевые принципы и архитектурные решения.

Служить основой для разработки более детальных документов: технического задания, частных политик, технических проектов.

Ключевые разделы Концепции создания КСЗИ:

1). Введение: Цели и задачи создания КСЗИ (например, снижение рисков до приемлемого уровня, соответствие требованиям законодательства).

2). Описание объекта защиты: Краткая характеристика IT-инфраструктуры организации.

3). Анализ угроз и модель нарушителя: Описание наиболее актуальных угроз (внешние, внутренние) и характеристика потенциальных нарушителей (их мотивация, возможности).

4). Защищаемые информационные активы: Перечень ключевых информационных ресурсов, подлежащих защите (например, ПДн клиентов, коммерческая тайна, финансовая информация).

5). Принципы построения КСЗИ: Фундаментальные подходы, которые будут заложены в систему (эшелонированная оборона, непрерывность защиты, централизованное управление, принцип минимальных привилегий).

6). Архитектура КСЗИ: Описание основных подсистем, из которых будет состоять КСЗИ (например, подсистема сетевой безопасности, антивирусной защиты, управления доступом, мониторинга и реагирования). Здесь описывается, что будет делать система, а не конкретные продукты.

7). Основные организационные меры: Описание ключевых организационных шагов для поддержки КСЗИ (создание отдела ИБ, разработка политик, обучение персонала).

8). Ожидаемые результаты: Что организация получит в итоге (управляемая система ИБ, минимизация ущерба от инцидентов, повышение доверия клиентов).

2. Порядок выполнения работы

1). Выберите вариант индивидуального задания.

2). Проанализируйте организацию из вашего варианта: ее бизнес-процессы, IT-инфраструктуру, ключевые активы и наиболее вероятные угрозы.

3). Разработайте проект Концепции создания КСЗИ для данной организации, используя структуру, описанную в теоретической части.

4). Наполните каждый раздел конкретным содержанием, исходя из специфики вашей организации. Уделите особое внимание разделам «Анализ угроз», «Принципы построения» и «Архитектура КСЗИ».

5). В разделе «Архитектура КСЗИ» опишите не менее 5-6 ключевых подсистем.

6). Напишите краткую пояснительную записку (2-3 абзаца), в которой обоснуйте, почему для данной организации были выбраны именно такие принципы и архитектурные решения.

7). Оформите результаты в виде проекта документа (3-4 страницы) и пояснительной записки.

3. Индивидуальные задания

Вариант 1. Организация: E-commerce маркетплейс

Крупная онлайн-площадка, соединяющая тысячи продавцов и миллионы покупателей. Инфраструктура полностью размещена в облаке. Принимаются онлайн-платежи. Основные риски: утечка ПДн и платежных данных, мошенничество, DDoS-атаки, взлом личных кабинетов.

Вариант 2. Организация: Научно-исследовательский институт (НИИ)

Институт, занимающийся передовыми разработками в области биотехнологий. Имеет собственную IT-инфраструктуру (серверы, сеть, рабочие станции). Основные риски: промышленный шпионаж с целью кражи интеллектуальной собственности (APT-атаки), утечка данных по вине инсайдеров, уничтожение результатов многолетних исследований.

Вариант 3. Организация: Система «Умный город»

Муниципальная система, управляющая городской инфраструктурой: светофорами, камерами видеонаблюдения, датчиками ЖКХ, общественным транспортом. Все данные стекаются в единый центр мониторинга. Основные риски: атаки на доступность (транспортный коллапс), манипуляция данными (подмена видеозаписей), нарушение приватности граждан.

III. РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

ТЕМЫ РЕФЕРАТОВ

1. Роль и место защиты информации в сфере информационных технологий.
2. Информация. Основные понятия и определения. Формы представления.
3. Классификация угроз информационной безопасности.
4. Охраняемые сведения и демаскирующие признаки.
5. Классификация технических каналов утечки информации.
6. Прямой акустический канал утечки информации.
7. Виброакустический канал утечки информации.
8. Акустоэлектрический канал утечки информации.
9. Акустооптический канал утечки информации.
10. Параметрический (акустический) канал утечки информации.
11. Электрический канал утечки информации.
12. Индукционный канал утечки информации.
13. Параметрический (электромагнитный) канал утечки информации.
14. Визуально-оптический и материально-вещественный каналы утечки информации.
15. Утечки информации по цепям заземления.
16. Утечки информации по цепям электропитания.
17. Перехват информации в телефонных каналах связи.
18. Классификация методов защиты информации.
19. Правовые методы защиты информации.
16. Организационные методы защиты информации.
17. Экранирование узлов и соединений аппаратуры.
18. Снижение уровней наводок на проводные тракты и узлы аппаратуры.
19. Звукоизоляция помещений.
20. Акустическая маскировка.
21. Электромагнитная маскировка.
22. Технические средства обнаружения закладных устройств.
23. Методы поиска и классификация работ по обнаружению и подавлению закладных устройств.
24. Категорирование объектов.
25. Классификация инженерно-технических методов защиты информации.
26. Инженерные заграждения.
27. Технические средства охраны периметра.
28. Охранное телевидение.
29. Системы контроля и управления доступом.
30. Политика безопасности.
31. Механизмы защиты автоматизированных систем.
32. Принципы реализации политики безопасности.
33. Аутентификация.
34. Рекомендации по использованию устройств аутентификации.

35. Принципы криптографической защиты информации.
36. Алгоритм шифрования ГОСТ 28147-89. Режим простой замены.
37. Электронно-цифровая подпись.
38. Защита транзакций в Internet.
39. Интеллектуальная собственность в развитии общества.
40. Авторское право и смежные права.
41. Промышленная собственность.
42. Объекты и субъекты авторского права и смежных прав.
43. Патентная информация.
44. Патентные исследования.
45. Введение объектов интеллектуальной собственности в гражданский оборот.
46. Коммерческое использование объектов интеллектуальной собственности.
47. Защита прав авторов и правообладателей.
48. Государственное управление интеллектуальной собственностью.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Основные законы, стандарты и рекомендации в области информационной безопасности.
2. Модель нарушителя.
3. Угрозы безопасности информационных технологий.
4. Анализ и управление рисками.
5. Политика информационной безопасности.
6. Документы, регламентирующие политику безопасности организации.
7. Стандарты построения систем информационной безопасности.
8. Организация и функционирование службы информационной безопасности.
9. Поведение оценки и разработка планов обработки рисков информационной безопасности.
10. Обучение и повышение осведомленности в области информационной безопасности.
11. Мониторинг, контроль защитных мер и аудит информационной безопасности.
12. Анализ функционирования системы обеспечения информационной безопасности.
13. Создание системы защиты информации.
14. Подготовка и аттестация системы защиты информации.
15. Эксплуатация системы защиты информации.
16. Модернизация системы защиты информации.
17. Управление инцидентами в области информационной безопасности.
18. Угрозы сетевой безопасности.
19. Межсетевые экраны.

20. Системы обнаружения и предотвращения вторжений.
21. Виртуальные частных сети.
22. Классификация объектов, подлежащих охране с помощью технических средств охраны.
23. Основные принципы оборудования объектов техническими средствами охранной сигнализации.
24. Понятие уровней защиты объекта.
25. Понятие рубежей охранной сигнализации.
26. Принципы работы приборов приемно-контрольных.
27. Принципы работы охранных извещателей, оповещателей, КТС.
28. Назначение систем цифровой регистрации видеосигнала.
29. Принципы работы видеокамер и устройств хранения видеоинформации.
30. Назначение систем контроля и управления доступом.
31. Принципы работы идентификаторов доступа, исполнительных устройств и устройств хранения информации.
32. Основные требования к инженерно-технической укрепленности объектов различных форм собственности.
33. Классификация инженерных заграждений и их назначение.
34. Инженерная защита дверных проемов зданий и въездных ворот объекта.

IV. ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие для студентов, обучающихся по направлению "Прикладная информатика" / Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. – М. : Риор : Инфра-М, 2019. – 335 с.

2. Вострецова, Е. В. Основы информационной безопасности : учеб. пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.

3. Николаев, Н. С. Управление информационной безопасностью : учебник для вузов / Н. С. Николаев. – М. : «КноРус», 2021. – 190 с.

4. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. – М. : Горячая линия. – Телеком, 2014.

5. Волынец-Руссет, Э. Я. Коммерческая реализация изобретений и ноу-хау (на внешних и внутренних рынках) : учебник / Э. Я. Волынец-Руссет. – М. : Экономист, 2004. – 326 с.

6. Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – М. : Горячая линия-Телеком, 2011. – 272 с.

7. Голиков, В. Ф. Безопасность информации и надежность компьютерных систем : учеб.-метод. пособие : в 2 ч. / В. Ф. Голиков. – Минск : БНТУ, 2010. – Ч. 1. – 90 с.

8. Голиков, В. Ф. Безопасность информации и надежность компьютерных систем : учеб.-метод. пособие : в 2 ч. / Голиков В.Ф. – Минск : БНТУ, 2012. – Ч. 2. – 84 с.

9. Гвоздек, М. Справочник по технике для видеонаблюдения. Планирование, проектирование, монтаж / М. Гвоздек. – М. : Техносфера, 2010. – 543 с.

10. Дашян, М. С. Интеллектуальная собственность в бизнесе: изобретение, товарный знак, ноу-хау, фирменный бренд / М. С. Дашян. – М. : Эксмо, 2010.

11. Деднев, М. А. Защита информации в банковском деле и электронном бизнесе / М. А. Деднев, Д. В. Дыльнов, М. А. Иванов. – М. : Кудиц-образ, 2004. – 512 с.

12. Зайцев, А. П. Технические средства и методы защита информации: учеб. пособие для ВУЗов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. – М. : Горячая линия – Телеком, 2012.

13. Лыньков, Л. М. Основы защиты информации и управление интеллектуальной собственностью: учеб.-метод. пособие / Л. М. Лыньков, В. Ф. Голиков, Т. В. Борботько. – Минск : БГУИР, 2013.

14. Рябенко, Б. Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябенко, А. Н. Фионов. – М. : Горячая линия – Телеком, 2013.

15. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – М. : Издат. дом «Форум» : Инфра-М, 2011. – 416 с.

16. Якимахо, А. П. Управление интеллектуальной собственностью в Республике Беларусь / А. П. Якимахо, Г. Е. Ясников, И. А. Рудаков; под ред. Г. Е. Ясникова. – Минск : Дикта, 2011.

17. Якимахо, А. П. Управление объектами интеллектуальной собственности в Республике Беларусь / А. П. Якимахо. – Минск : Амалфея, 2005. – 472 с.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

1. Концепция национальной безопасности Республики Беларусь : решение Всебелорусского народного собрания от 25 апр. 2024 года № 5 // Национальный правовой Интернет-портал Республики Беларусь. – URL: https://pravo.by/document/?guid=12551&p0=P924v00051 (дата обращения: 11.03.2025).

2. О некоторых вопросах развития информационного общества в Республике Беларусь : Указ Президента Респ. Беларусь от 08 нояб. 2011 г. № 515 : в ред. от 22 июня 2023 г. № 178 // ЭТАЛОН : информ.-поисковая система (дата обращения: 11.03.2025).

3. О Концепции информационной безопасности Республики Беларусь : постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1 // ЭТАЛОН : информ.-поисковая система (дата обращения 12.03.2025).

4. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008г. № 455-З: в ред. от 10.10.2022№209-З // ЭТАЛОН : информ.-поисковая система (дата обращения 12.03.2025).

5. Охрана объектов и физических лиц. Термины и определения : СТБ 1250-2000. – Введ. 01.04.2001. – Минск : БелГИСС, 2000. – 20 с.

6. Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах : СТБ 34.101.70-2016. – Введ. 01.04.2017. – Минск : НИИ ТЗИ, 2016. – 40 с.

7. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: СТБ ISO/IEC 27001-2016. – Введ. 01.10.2016 (с отменой на территории СТБ ISO/IEC 27001-2011). – Минск : БелГИСС, 2016. – 28 с.

8. Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности: СТБ ISO/IEC 27003-2014. – Введ. 01.02.2015. – Минск : НИИ ТЗИ, 2014. – 68 с.

9. Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности: СТБ КОЯЕС 27005-2012. – Введ. 01.01.2013. – Минск : БелГИСС, 2012. – 68 с.

10. Охрана объектов. Требования по применению технических средств и систем охраны: ТКИ № 627-2018 (33030). – Введ. 01.01.2019 (с отменой на территории РБ РД 28/3.006-2005). – Минск : ДО МВД РБ, 2018. – 18 с.

11. Охрана объектов. Охрана объектов. Обеспечение технической укрепленности объектов: ТКП 652-2020 (33030). – Введ. 01.01.2021 (с отменой на территории РБ РД 28/3.012-2005). – Минск : Стройтехнорм, 2020. – 55 с.