Методические рекомендации по подготовке к прохождению практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал»

(номинация «Кадетский класс»,
направление «Государственная служба российского казачества (Казаки)»)

Москва
2024

Методические рекомендации по подготовке к прохождению практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» (в номинации «Кадетский класс» по направлению «Государственная служба российского казачества (Казаки)»).

Предпрофессиональная профильная подготовка обучающихся кадетских классов нацелена на формирование личности патриота Отечества, обладающего высоким уровнем профессионального мастерства, готового стать надежной опорой государства.

Конкурс межпредметных навыков и знаний является формой итоговой проверки уровня освоения обучающимися образовательной организации дополнительных общеобразовательных общеразвивающих программ с учетом профиля кадетской подготовки.

В ходе проведения практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» (в номинации «Кадетский класс» по направлению «Казаки») обучающимся предлагается выполнить практические задания, почувствовав себя в роли специалиста по защите информации. Каждому обучающемуся выдается заранее подготовленный информационный материал (включающий графику и текст) и извлечение из законодательства РФ, связанное с выявлением противоправного (запрещенного) контента о наркотических веществах, суициде, экстремистской деятельности и т.д. Выданный обучающемуся материал не является реальным противоправным Интернет-контентом, но наглядно показывает отдельные элементы, позволяющие идентифицировать подобные материалы.

Методические рекомендации подготовлены в рамках организации и проведения практической части Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» (в номинации «Кадетский класс» по направлению «Государственная служба российского казачества (Казаки)»).

В текст рекомендаций вошли методические и практические материалы, подготовленные на основе опыта организации работы молодежных кибердружин и киберотрядов.

СОДЕРЖАНИЕ

ЦЕЛИ И ЗАДАЧИ ПРАКТИЧЕСКОГО ЭТАПА КОНКУРСА

Целью прохождения практического этапа конкурса межпредметных навыков и знаний является ознакомление обучающихся с представления о безопасности в информационном обществе, формирование на данной основе понимания технологий практического этапа защиты информации и умения применять эти технологии во всех сферах деятельности, в том числе для защиты государства, общества и личности.

Задачами практического этапа являются:

- ознакомить обучающихся с основными понятиями информационной безопасности и средствами защиты от основных видов угроз;
- рассмотреть возможные методы программно-аппаратной зашиты информации, а также несколько видов криптографической защиты;
- выделить ключевые проблемы сохранения национальной безопасности России в условиях информационной войны;
- совершенствовать школьное образование и подготовку в сфере информационных технологий;
- способствовать популяризации профессий, связанных с информационной безопасностью и информационными технологиями в целом.

В результате прохождения обучения перед прохождением практического этапа конкурса предпрофессиональных умений обучающиеся должны **знать**:

- основные понятия и определения информационной безопасности
- основные виды угроз в современном информационном пространстве;
- принципы функционирования систем защиты информации;
- наиболее распространённые виды киберпреступлений и правовые аспекты защиты киберпространства;
- понятие «информационная война» и виды информационного оружия;
- основные положения государственной политики в области информационной безопасности.

Обучающиеся должны **уметь**:

- соблюдать нормы информационной этики и права;
- просчитывать угрозы безопасности государства, общества и личности в современном информационном пространстве;
- выявлять признаки работы компьютерных вирусов и использовать антивирусное программное обеспечение;
- определять специфику угроз информационной безопасности в различных сферах деятельности;
- использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением

требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Спецификация конкурсных материалов для проведения практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» в номинации «Кадетский класс» по направлению «Казаки»

1. Назначение конкурсных материалов

Материалы практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» (далее – Конкурс) предназначены для оценки уровня практической подготовки участников Конкурса освоивших программу подготовки в рамках проекта «Кадетский класс в московской школе» по направлению «Казаки».

2. Условия проведения

Практический этап Конкурса проводится в дистанционной форме – в форме компьютерного тестирования. При выполнении работы обеспечивается строгое соблюдение порядка организации и проведения Конкурса.

3. Продолжительность выполнения

На выполнение заданий практического этапа Конкурса отводится 60 минут.

4. Содержание и структура

Задания практического этапа Конкурса разработаны преподавателями образовательных организаций высшего образования, участвующих в проекте «Кадетский класс в московской школе». Индивидуальный вариант участника формируется автоматически во время проведения практического этапа Конкурса предпрофессиональных умений из базы конкурсных заданий. Индивидуальный вариант участника включает 15 заданий, базирующихся на содержании рабочих программ, «Военная история для кадетских классов», «Основы информационной безопасности для кадетских классов». Индивидуальный вариант участника включает *15 заданий*: 10 заданий базового уровня и 5 задания продвинутого уровня.

5. Система оценивания

Задание –считается выполненным, если ответ участника совпал с эталоном. Каждое верно выпаленное задание базового уровня максимально оценивается в 3 балла, каждое верно выполненное задание повышенного уровня максимально оценивается в 6 балла.
Максимальный балл за выполнение всех заданий – 60 баллов. Для получения максимального балла за практический этап Конкурса необходимо дать полные верные ответы на все 15 заданий: 10 заданий базового и 5 заданий продвинутого уровней.

6. Приложения

1. План конкурсных материалов для проведения Конкурса.

2. Демонстрационный вариант конкурсных заданий практического этапа Конкурса.
3. Подготовительные материалы к заданиям

Приложение 1

План конкурсных материалов для проведения Конкурса

№ критерия	Уровень сложности	Темы	Контролируемые требования к проверяемым умениям	Балл
1.	базовый	Введение в информационную безопасность. Основные понятия. Угрозы в информационной безопасности. Основные виды.	уметь толковать и понимать основные понятия, информационной безопасности	3
2.	базовый	Технические средства защиты информации и основные каналы утечки.	умение работать с техническими средствами защиты информации	3
3.	базовый	Защита информационных систем.	уметь без грамматических и смысловых ошибок письменно формулировать ответ	3
4.	базовый	Основные методы и средства	умение описать варианты воздействий и способы защиты	3
5.	базовый	Основные нормативные руководящие документы информационной безопасности. Понятие государственной тайны, Виды секретности.	Умеет анализировать и применять нормы права, стандарты, техническую документацию при решении задач профессиональной деятельности.	3
6.	базовый	Уголовный и административный кодекс правонарушений. Ответственность в сфере информационной безопасности	Умение выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений	3
7.	базовый	Международные стандарты в сфере информационной безопасности	умение ориентироваться в международных стандартах в сфере информационной безопасности	3
8.	базовый	Военные конфликты накануне Великой Отечественной войны, Зимне-весенняя военная кампания 1945 года, Летне-осенняя военная кампания 1944 года, Зимне-весенняя военная кампания 1944 года, Военные реформы периода Великой Отечественной войны, Летне-осенняя кампания 1943 года,	Умение анализировать задачу, используя основы критического анализа и системного подхода	3

		Зимне-весенняя военная кампания 1942-1943 годов, Участие России в I мировой войне., Русско-японская война 1904-1905 годов. Оборона Порт-Артура Военная кампания 1914 года		
9.	базовый	Публикация персональной информации, Приватность и конфиденциальность в сети. Фишинг	Умение описать процедуру публикации персональной информации, защиты аккаунта в сети, умение разрабатывать и оценивать альтернативные решения с учетом рисков	3
10.	базовый	Войны XVI века и развитие военного дела, Военные реформы до и после распада СССР, Региональные и этнические конфликты на территории бывшего СССР в конце XX века. Система коллективной безопасности на постсоветском пространстве, Основные направления современного строительства вооруженных сил РФ, Чеченские войны и военные конфликты начала XXI века. Деятельность ОДКБ, Военное образование в России начала XXI века: основные направления и перспективы развития, Война в Афганистане 1979-1989 годов, Организация Варшавского договора: условия, руководящие органы, деятельность, Военные конфликты конца 1940-1950 годов. Война в Корее 1953-1955 годов, Положение Вооружённых Сил СССР после Великой Отечественной войны. Развитие Вооруженных Сил СССР в 1945-1965 годы	Умение запоминать значимые события, относящиеся к истории ведомств	3
11.	расширенный	Варианты воздействия и способы защиты. Социальная инженерия. Правила безопасности при общении в сети. Безопасность аккаунтов в сети.	Умение анализировать предложенную текстовую информацию. Умение формировать собственные суждения и оценки, грамотно и логично аргументируя свою точку зрения	6

12.	расширенный	Безопасность аккаунтов в сети. Совершение покупок онлайн	Умение анализировать предложенную текстовую информацию. Умение сопоставлять и оценивать различные варианты решения поставленной задачи, определяя их достоинства и недостатки	6
13.	расширенный	Система как объект информационных воздействий и управления	Умение анализировать предложенную текстовую информацию. умение проводить основные работы при эксплуатации технических средств защиты информации	6
14.	расширенный	Концепция сетецентрической и информационной войны	Умение формировать собственные суждения и оценки, грамотно и логично аргументируя свою точку зрения	6
15.	расширенный	Информационное противоборство в психологической сфере. Когнитивная самооборона в условиях информационного противоборства	Умение проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений	6
			Сумма баллов:	**60**
			Из них: от 0 до 30 баллов – **базовый уровень** от 31 до 60 баллов – **расширенный уровень**	

Приложение 2

Демонстрационный вариант конкурсных заданий практического этапа Конкурса

Пример состава задания практического этапа Конкурса.

ВАРИАНТ 1 (демовариант)

Задание базовой сложности.

Задание №1.

Согласно Федеральному закону от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации» информация это:

1) сведения (сообщения, данные) независимо от формы их представления;
2) некоторое сообщение в цифровом виде;
3) вербальные (словесные, звуковые) данные
4) кодированное сообщение.

Ответ: 1)

3 балла за верный ответ.

Задание №2.

Согласно Федеральному закону от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации» информационная система это:

1) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
2) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
3) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
4) часть сайта в сети "Интернет".

Ответ: 3)

3 балла за верный ответ.

Задание №3.

Согласно Указу Президента Российской Федерации от 05.12.2016 г. № 646

«Об утверждении Доктрины информационной безопасности Российской Федерации»
Информационная безопасность Российской Федерации это:

1) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;
2) государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;
3) осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

Ответ: 1)

3 балла за верный ответ.

Задание №4.

Отметить правильный варианта ответа:

Информационная безопасность подразделяется на

1) Организационно-правовую
2) Программно-аппаратную
3) Криптографическую
4) Информационно – аналитическую
5) Психологическую.
6) Инженерно –техническую

Ответ: 1), 2), 6)

3 балла за верный ответ.

Задание №5.

Как называлась переносная шифровальная машина, использовавшаяся нацисткой Германией для шифрования и дешифрования секретных сообщений во время Второй мировой Войны, представленная на рис.1:

1) Лоренц
2) Энигма
3) R732
4) Colossus

Рис.1

Ответ: 2)

3 балла за верный ответ.

Задание №6.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера (рис.2). Применительно к русскому алфавиту таблица Виженера составляется из строк по 33 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 33 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Задание: Согласно принципу дешифрования, определить крупнейшее сражение Отечественной войны 1812 года.

Ключ: Кутузов

Исходный текст: «Лвгвлчпьютт ичфму»

	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
В	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ё	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё
З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж
И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Ю	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Я	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Рис.2

Ответ: Бородинское сражение.

3 балла за верный ответ.

Задание №7.

Согласно закону РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2023) "О государственной тайне" дайте определение понятию государственная тайна

Государственная тайна - это

Ответ: Это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

3 балла за верный ответ.

Задание № 8.

Дайте определение техническому каналу утечки информации (ТКУИ)

Ответ:

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

3 балла за верный ответ.

Задание № 9.

Для чего применяется электромагнитное экранирование технических систем и информационный цепей?

Ответ: Для защиты технических систем от утечки информации по параметрическим каналам связи.

3 балла за верный ответ.

Задание повышенной сложности.

Здание №10.

Для блокирования угроз, исходящих из общедоступных систем, используется специальное программное или аппаратно-программное средство – межсетевой экран (Firewall). Опишите 4 основные функции, которые он выполняет:

1)

2)

3)

4)

Ответ:

1) Фильтрация трафика

2) Использование экранирующих агентов
3) Трансляция адресов
4) Регистрация событий

6 баллов за верный ответ.

Задание №11.

К настоящему времени компьютерная вирусология накопила определенную историю, которую в вкратце можно проиллюстрировать следующими основными эпизодами: Установите соответствие год - произошедшее событие

a) 1987 г.
b) 1988 г.
c) 1981-1982г.
d) 1985 – 1986 г.
e) 1951г.
f) 1980 г.

1) Публикация Джона фон Неймана, в которой исследовалась проблема создания саморазмножающихся компьютерных программ
2) Первая европейская публикация о компьютерных вирусах «Самовоспроизводящиеся программы» И. Краузе, содержащая листинги вирусов на языке Ассемблера
3) Появился первый бутовый вирус (Elk Cloner)
4) Вспышки заражения компьютерными вирусами многих персональных компьютеров, причиной которых стало бесконтрольное копирование файлов
5) Появление вируса Vienna
6) Эпидемия сетевого вируса Морриса

Ответ:

1951 г. – 1)

1980 г. - 2)

1981-1982г. – 3)

1985 – 1986 г. – 4)

1987г. – 5)

1988 г. – 6)

6 баллов за верный ответ.

Задание №12.

Дополните список ниже основными принципами инженерно-технической защиты информации.

1) надежность защиты информации;
2)
3)
4) целеустремленность защиты информации;
5) рациональность защиты;
6)
7) гибкость защиты информации;
8)
9) комплексное использование различных способов и средств защиты информации;
10)

Ответ: Дополнить не важно в каком порядке

непрерывность защиты информации, экономичность защиты информации, скрытность защиты информации, многообразие способов защиты, активность защиты информации;

6 баллов за верный ответ.

Задание **№**13.

Перед вами таблица классов защищенности автоматизированной системы управления (АСУ). Необходимо правильно соотнести уровень значимости (критичности) УЗ, с классом защищенности

Уровень значимости (критичности) информации присваивается		Класс защищенности автоматизированной системы управления	
УЗ1	если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена высокая степень ущерба	КС1	
УЗ2	если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.	КС2	
УЗ3	если для всех свойств безопасности информации (целостности, доступности, конфиденциальности) определены низкие степени ущерба.	КС3	

1) Осуществляет нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом.
2) Осуществляет нейтрализацию (блокирование) угроз безопасности

информации, связанных с действия нарушителя с низким потенциалом

3) Осуществляет нейтрализацию (блокирование) угроз безопасности информации, связанных с нарушителем с потенциалом не ниже среднего.

Ответ: По порядку сверху вниз 1, 3, 2.

6 баллов за верный ответ.

Задание №14

Установите соответствие наименования и описания международных стандартов в области ИБ

a) BS 7799-3:2006 —

b) BS 7799-2:2005 —

c) BS 7799-1:2005 —

d) ISO/IEC 17799:2005 —

e) BS 7799-2:2005 —

f) ISO/IEC 27002 —

g) ISO/IEC 27005 —

1) Британский стандарт Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров

мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ

2) Британский стандарт Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.
3) Британский стандарт третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности
4) «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.
5) Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
6) Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.

Ответ:

BS 7799-1:2005 — 1)
BS 7799-2:2005 — 2)
BS 7799-3:2006 — 3)
ISO/IEC 17799:2005 — 4)
ISO/IEC 27001 — 5)
ISO/IEC 27005 — 6)

6 баллов за верный ответ.

Задание №15

Перечислите основные технические каналы утечки информации
Ответ:

1) Электромагнитные
2) Индукционные
3) Гальванические

4) Параметрические
5) Аппаратные закладки

6 баллов за верный ответ.

Список литературы и источников:

1) Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации»
2) Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
3) М.А. Борисов, И.В. Заводцев, И.В. Чижов «Основы программно-аппаратной защиты информации», изд. 4-е, 2016 г.
4) Закон РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2023) "О государственной тайне"
5) Расторгуев С. П. Абсолютная система защиты // Системы безопасности, связи и телекоммуникаций. — 1996.
6) Поздняков Е. Н. Защита объектов (Рекомендации для руководителей и сотрудников служб безопасности). — М.: Банковский Деловой Центр, 1997.
7) В.П. Мельников, С.А. Клейменов, А.М. Петраков «Информационная безопасность» 2005 г.
8) А.И. Куприянов, А.В. Сахаров, В.А. Шевцов «Основы защиты информации» 2006 г.
9) А.А. Хорев «Защита информации от утечки по техническим каналам» 1998 г.

ОСНОВНЫЕ МАТЕРИАЛЫ ДЛЯ ПОДГОТОВКИ К ПРОХОЖДЕНИЮ ПРАКТИЧЕСКОГО ЭТАПА КОНКУРСА

ОСНОВНЫЕ ПОНЯТИ И ОПРЕДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для удобства обучающихся материалы методических материалов разделены на два раздела: основные и дополнительные материалы, приведенные в Приложении №3 настоящих методических рекомендаций.

Основные материалы описывают структуру кейс-заданий практического этапа конкурса и дают базовые знания, требуемые для их решения.

Дополнительные материалы дают более глубокое представление об информационной безопасности, программно-аппаратной защите информации, правовых аспектах защиты информации и информационном законодательстве РФ. Эти материалы не являются обязательными при решении кейс-заданий, но применение использованной в них терминологии в ответе на кейс-задание может помочь получить более высокий балл.

Изучение основных понятий и определений информационной безопасности.

Информация в настоящее время является движущим фактором развития общества. Наличие достоверной и актуальной информации позволяет управлять производственными и организационными процессами, влиять на социум. Все более важную роль в жизни общества играют различные информационные и коммуникационные технологии (ИКТ), информационные системы (ИС), базы данных (БД) и др. Их уязвимость обостряет необходимость наличия определенных знаний и навыков по защите информации, что при отсутствии знаний в данной области приведет к значительным потерям. Все вышеперечисленное повлияло на то, что информационная безопасность (ИБ) стала одной из главных проблем, с которой сталкивается современное общество, и ее значимость будет только увеличиваться по мере развития ИКТ и увеличения масштабов их внедрения.

Согласно Доктрине информационной безопасности РФ, обеспечение информационной безопасности Российской Федерации является ключевым

фактором в обеспечении национальной безопасности. При этом одним из ведущих направлений является совершенствование подготовки кадров и развитие образования в области информационной безопасности.

Освоение новой области знаний должно начинаться с основных понятий и определений. Одним из ключевых определений при изучении основ ИБ является собственно определение информационной безопасности, однако в настоящее время оно не имеет однозначной формулировки.

Например, согласно ГОСТ Р 50922-2006, безопасность информации (данных) – это состояние защищенности информации (данных), при котором обеспечены её (их) конфиденциальность, доступность и целостность, а защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

В другом государственном стандарте – ГОСТ Р ИСО/МЭК 17799-2005 – информационная безопасность определяется как защита конфиденциальности, целостности и доступности информации, где конфиденциальность – это свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц; целостность – это неизменность информации в процессе ее передачи или хранения; доступность – это свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

В Доктрине информационной безопасности Российской Федерации под информационной безопасностью подразумевается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Анализируя приведенные выше определения, можно прийти к выводу, что словосочетание «информационная безопасность» в разных контекстах имеет различный смысл. В контексте данных заданий будем придерживаться определения из Доктрины ИБ РФ. Так же приведем несколько основных определений из Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации»

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Основные свойства информации

Рассмотрим более подробно свойства информации:

1. Конфиденциальность – защита от несанкционированного ознакомления. Это уверенность создателя или владельца информации в том,

что никто не сможет получить к ней доступ без его ведома. Пример: вы написали записку вашей подруге и не хотите, чтобы с её содержанием ознакомились посторонние. В этом случае вам важна именно конфиденциальность информации.

2. Целостность – актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения. Это признак того, что информация не будет изменена без ведома автора. Например, вы заключили с кем-то договор на 15 тысяч рублей и не хотите, чтобы в договоре появилась какая-то другая сумма. Вам важна целостность этого договора, его неизменность.

3. Доступность - возможность за приемлемое время получить требуемую информацию. Это свойство информации, означающее вашу уверенность в том, что вы найдете ваши данные там, где вы их оставили. Например, если вы положили важный документ в ящик стола и не хотите, чтобы его кто-то брал, значит, для вас важна доступность этой информации.

Эти примеры отражают аспекты защиты информации - обеспечение конфиденциальности, целостности, доступности - и являются главной целью и задачей информационной безопасности.

Угрозы в информационной безопасности. Основные виды.

Под угрозой безопасности информации (информационной угрозой) понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Все множество потенциальных угроз информационной безопасности по природе их возникновения можно разделить на два класса:

- естественные (объективные);
- искусственные (субъективные).

К естественным относятся природные явления, которые не зависят от человека, например, ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и

изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации. Классификация угроз информационной безопасности В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы.

1. Нежелательный контент;
2. Несанкционированный доступ;
3. Утечки информации;
4. Потеря данных;
5. Мошенничество;
6. Кибервойны;
7. Кибертерроризм.

Технические средства защиты информации и основные каналы утечки.

Средства защиты информации – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Согласно ГОСТ Р 50922-2006 средство защиты информации – это техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Под **техническим каналом утечки информации** (ТКУИ) понимают совокупность источника информации (передатчика), линии связи (физической среды – канал с шумами), по которой распространяется информационный сигнал, и технических средств перехвата информации (приемника).

Защита информационных систем

Под защитой информации в информационных системах понимается регулярное использование в них средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения требуемой надежности информации, хранимой и обрабатываемой с использованием средств информационных систем.

Предприятие начинается с его собственной безопасности и, в первую очередь, это физическая защита. К ней можно отнести системы контроля

доступа, охранные видеокамеры, датчики, системы сигнализации и др. Мир физической безопасности понятен любому человеку, в том числе и руководству предприятия.

При выборе стратегии защиты информационных систем можно рассматривать, что информационная система – это тоже своего рода здание, только виртуальное, которое необходимо защищать. Использовать для этого можно те же механизмы физической безопасности, но спроецированные с учетом информационных технологий. Например, вход в обычное здание блокируется охранником или турникетом. В виртуальном здании для этого используется межсетевой экран или система аутентификации, которые проверяют входящий и исходящий в систему график на соответствие заданным критериям. Злоумышленник для несанкционированного проникновения в здание может подделать пропуск (в виртуальном мире подделать адрес) или пролезать через окно (в виртуальном мире через модем). Здесь мы рассмотрим наиболее важные объекты защиты в информационных системах. Это защита персонального компьютера и защита информации в сетях ЭВМ.

1. Защита пк от несанкционированного доступа

Как показывает практика, несанкционированный доступ (НСД) представляет одну из наиболее серьезных угроз для злоумышленников завладения защищаемой информацией в современных информационных системах. Как ни покажется странным, но для ПК опасность данной угрозы по сравнению с большими ЭВМ повышается, чему способствуют следующие объективно существующие обстоятельства:

1) подавляющая часть ПК располагается непосредственно в рабочих комнатах специалистов, что создает благоприятные условия для доступа к ним посторонних лиц;

2) многие ПК служат коллективным средством обработки информации, что обезличивает ответственность, в том числе и за защиту информации;

3) современные ПК оснащены несъемными накопителями на ЖМД очень большой емкости, причем информация на них сохраняется даже в обесточенном состоянии;

4) накопители на ГМД производятся в таком массовом количестве, что уже используются для распространения информации так же, как и бумажные носители;

5) первоначально ПК создавались именно как персональное средство автоматизации обработки информации, а потому и не оснащались специально средствами защиты от НСД.

В силу сказанного те пользователи, которые желают сохранить конфиденциальность своей информации, должны особенно позаботиться об оснащении используемой ПК высокоэффективными средствами защиты от НСД.

Основные механизмы защиты ПК от НСД могут быть представлены следующим перечнем:

1) физическая защита ПК и носителей информации;
2) опознавание (аутентификация) пользователей и используемых компонентов обработки информации;
3) разграничение доступа к элементам защищаемой информации;
4) криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);
5) криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки;
6) регистрация всех обращений к защищаемой информации.

Содержание физической защиты общеизвестно, поэтому детально обсуждать ее здесь нет необходимости. Заметим только, что ПК лучше размещать в надежно запираемом помещении, причем, в рабочее время помещение должно быть закрыто или ПК должен быть под наблюдением законного пользователя. При обработке закрытой информации в помещении могут находиться только лица, допущенные к обрабатываемой информации. В целях повышения надежности физической защиты в нерабочее время ПК следует хранить в опечатанном сейфе.

Защита информационных систем

Главным нормативным документом, который дает определение разным видам информации и регулирует ее применение, является Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации» от 27.06.2006 г. (последняя редакция от 18.03.2019). Согласно ст. 9 этого закона, ограничение доступа к информации устанавливается федеральными законами в целях охраны основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

При этом требования об ограничениях доступа к сведениям разрабатываются и контролируются специальным органом исполнительной власти, на который возлагаются функции по надзору в сфере информационных технологий и массовых коммуникаций.

Законом охраняется также право на нераспространение информации о личной жизни физического лица (гражданина), поскольку такие сведения относятся к категории семейной тайны.

К отдельной категории относится информация, составляющая государственную тайну, поэтому многие служащие перед поступлением на работу подписывают соответствующие документы о неразглашении данных. Охрана такой информации осуществляется согласно закону Российской Федерации «О государственной тайне» от 21.07.1993 № 5485-1, по которому к категории государственной тайны относятся сведения по следующим направлениям:

- экономика, наука и техника;
- военная промышленность и вооружение;
- внешняя и внутренняя политика;
- сведения в области разведывательной и контрразведывательной деятельности.

Если говорить о конфиденциальной информации, полный ее перечень изложен в Указе Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». Документ относит к ним следующие виды информации:

1. Персональные данные гражданина.
2. Сведения, которые составляют тайну следствия и судопроизводства.
3. Служебные данные.
4. Информация о сущности изобретения (полезная модель, экспериментальная установка, промышленный образец).
5. Профессиональная тайна.

Важно понимать, что информацию с ограниченным доступом следует хранить особым образом, исключая риск ее попадания к третьим лицам, поскольку это может привести к утечке секретных данных, а также причинить ущерб или вред государству, личности или коммерческой фирме. По этой причине охране информации от хищения, искажения и незаконного распространения уделяют повышенное внимание, используя для этого специальные системы контроля, ограничивающие доступ.

Способы охраны информации в корпоративных системах

Все организации, начиная с самых маленьких фирм и заканчивая большими государственными корпорациями, нуждаются в особо тщательной охране внутренней информации. Это обусловливается высоким уровнем недобросовестной конкуренции и промышленным шпионажем, когда похищенные сведения в виде чертежей, проектов, инновационных разработок

и финансовых данных приводят к экономическим убыткам. В связи с этим особую актуальность приобретают меры, направленные на защиту информации от несанкционированного копирования.

Существуют разные способы и методы защиты конфиденциальной информации, к которой также относят различные виды тайн (судебная, медицинская, банковская, нотариальная). Выделяют три главных группы мер по защите информации, каждую из которых следует рассмотреть подробнее.

Организационно-юридические меры

Ограничения доступа к конфиденциальной информации на предприятии начинается с разработки руководящим составом ряда нормативно-правовых актов, направленных на упорядочивание имеющейся документации. С этой целью выделяются разные категории сотрудников с доступом к важной информации в зависимости от должности и должностных обязанностей. К документам, регламентирующим обращение с критичными данными, относятся приказы, распоряжения, методические указания, регламенты и всевозможные инструкции, направленные на упорядочивание бизнес-процессов с целью повышения эффективности и выхода на максимальную доходность.

Главным правовым документом, который регламентирует соблюдение коммерческой тайны, является Федеральный закон № 98 «О коммерческой тайне» от 29.07.2004 года, контроль за выполнением которого возлагается на ФСТЭК и ФСБ. Если говорить об охране персональных данных, то она регламентируется Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ. Контроль за выполнением возлагается на Роскомнадзор.

Нужно понимать, что у любой фирмы имеется информация, которая может представлять интерес для третьих лиц, поэтому руководителю важно принимать все меры, исключающие риск ее передачи. Необходимость точного регламентирования всей информации обусловливается еще и тем, что рядовые сотрудники могут передать сведения о фирме другому участнику информационного обмена неумышленно. Отсутствие на предприятии утвержденного перечня информации, относящейся к категории служебной или государственной тайны, делает невозможным привлечение сотрудника, передавшего информацию третьему лицу, к дисциплинарной ответственности.

Инженерно-технические меры

Учитывая повсеместное использование электронных носителей данных, для охраны конфиденциальной информации требуются технические средства, ограничивающие ее копирование, передачу и искажение.

Выделяют четыре группы защитных мер:

1. **Предотвращение несанкционированного доступа.**

Является эффективным средством от попадания данных в чужие руки, поскольку не допускает посторонних к их обработке. Комплекс мер по защите включает межсетевое экранирование, систему контроля управления доступом (логин и пароль), учет и регистрацию входов (журналирование), антивирусную защиту и использование средств обнаружения вторжений.

2. **Инженерно-технические ограничения.**

Немало злоумышленников осуществляют кражу важной информации путем несанкционированного вторжения на территорию компании. С целью недопущения таких инцидентов на предприятиях устанавливаются специальные инженерно-технические сооружения: турникеты, сигнализации, системы видеонаблюдения и кодовые замки. К данным средствам также относят противопожарные комплексы, способные не только оповестить о задымлении, но и потушить очаг возгорания, обеспечив сохранность серверной и рабочих мест.

3. **Защита от утечек информации по техническим каналам.**

Главная задача – не допустить передачи сведений при помощи электромагнитных считывателей информации доступа. С этой целью на предприятии применяются шторы-жалюзи, виброакустические глушилки, специальные фильтры для защиты от побочных электромагнитных наводок и излучений. С каждым годом актуальность использования подобных решений увеличивается, что обусловливается ценовой доступностью техсредств для потенциальных шпионов.

4. **Криптографические средства.**

Необходимы для охраны информации во время ее передачи по электронным каналам связи. Учитывая широкое распространение электронного документооборота, криптографические средства имеют важное значение. С целью дополнительной защиты информации от искажения, а также подтверждения ее авторства используется электронная подпись. Механизм криптографической защиты применяется для обеспечения конфиденциальности информации, хранимой в базе, и реализуется путем построения VPN-сетей (Virtual Private Network).

Чтобы защитить конфиденциальную информацию, важно своевременно модернизировать имеющиеся инженерно-технические комплексы на предприятии, поскольку только таким образом можно снизить риски хищения данных до минимума.

Морально-этические меры

Практика подтверждает, что в большинстве случаев утечки случаются по вине людей, работающих на предприятия. Именно поэтому с каждым годом все больше компаний при приеме на работу новых людей подписывают с ними договор о неразглашении конфиденциальных данных. Согласно данным исследования аналитического центра «СёрчИнформ», в 2018 году такие договоры практикует 81% российских компаний. В большинстве случаев распространение данных не связано с умышленными действиями и объясняется беспечностью или необдуманными поступками сотрудников предприятия. По этой причине важно правильно подбирать персонал на ответственные должности, а также периодически проводить обучение сотрудников ИБ-правилам.

Морально-этические меры по защите информации напрямую связаны с кадровой безопасностью, для чего на предприятии должны быть заведены журналы инструктажей, разработаны соответствующие должностные инструкции, включающие в себя порядок ознакомления с информацией, составляющей коммерческую тайну. При увольнении сотрудников также следует принимать соответствующие меры безопасности, изымая удостоверения и пропуски, аннулируя пароли доступа, а также беря подписку о неразглашении данных.

Служба безопасности (внутреннего контроля) предприятия должна отслеживать сотрудников с целью выявления тех, кто опаздывает на работу, уходит раньше положенного времени, проводит много часов за играми или в социальных сетях (в рабочее время), что свидетельствует о низком уровне ответственности таких «специалистов». С целью активного мониторинга и выявления всех факторов риска во многих компаниях используются специальные программы, позволяющие выявлять тех сотрудников, поведение которых отклоняется от нормы.

В каждой компании имеются сведения, которые составляют коммерческую тайну, поэтому ограниченный доступ к информации – не рекомендуемая, а необходимая мера безопасности. К сожалению, в большинстве случаев сотрудники не до конца осознают важность сохранения конфиденциальной информации в тайне, а также необходимость устанавливать сложные пароли и логины. Более того, нередко усиленные меры, принимаемые руководством компании для защиты информации, воспринимаются сотрудниками как некомфортные, ведь для их реализации работникам необходимо соблюдать процедуру входа в систему и другие внутренние ИБ-правила. Вместе с тем руководитель должен понимать, что

ограниченный доступ – это важнейшая мера безопасности, направленная на предотвращение утечек данных.

Определение класса защищенности автоматизированной системы управления (АСУ ТП)

Определение класса защищенности государственной информационной системы осуществляется в соответствии с приказом ФСТЭК РФ от 14 марта 2014 г. № 31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды"

Класс защищенности автоматизированной системы управления (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости (критичности) обрабатываемой в ней информации (УЗ).

Уровень значимости (критичности) информации (УЗ) определяется степенью возможного ущерба от нарушения ее целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), в результате которого возможно нарушение штатного режима функционирования автоматизированной системы управления или незаконное вмешательство в процессы функционирования автоматизированной системы управления.

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, степень ущерба)],

где степень возможного ущерба определяется заказчиком или оператором экспертным, или иным методом и может быть:

- высокой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации федерального или межрегионального характера* или иные существенные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;
- средней, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности),

повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации регионального или межмуниципального характера* или иные умеренные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

- низкой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации муниципального (локального) характера или возможны иные незначительные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности.

В случае, если для информации, обрабатываемой в автоматизированной системе управления, не требуется обеспечение одного из свойств безопасности информации (в частности конфиденциальности) уровень значимости (критичности) определятся для двух других свойств безопасности информации (целостности, доступности). В этом случае:

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, не применяется)].

Информация, обрабатываемая в автоматизированной системе управления, **имеет высокий уровень значимости (критичности) (УЗ 1)**, если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена высокая степень ущерба.

Информация, обрабатываемая в автоматизированной системе управления, имеет **средний уровень значимости (критичности) (УЗ 2)**, если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Информация, обрабатываемая в автоматизированной системе управления, имеет **низкий уровень значимости (критичности) (УЗ 3)**, если для всех свойств безопасности информации (целостности, доступности, конфиденциальности) определены низкие степени ущерба.

При обработке в автоматизированной системе управления двух и более видов информации (измерительная информация, информация о состоянии процесса) уровень значимости (критичности) информации (УЗ) определяется отдельно для каждого вида информации. Итоговый уровень значимости

(критичности) устанавливается по наивысшим значениям степени возможного ущерба, определенным для целостности, доступности, конфиденциальности каждого вида информации.

Организационно – правовое обеспечение ИБ

Федеральные законы, указы и постановления правительства в области ИБ:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации
- Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»
- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
- Указ Президента Российской Федерации от 03 апреля 1995 г. N 334
- Указ Президента Российской Федерации от 17 марта 2008 г. N 351
- Постановление Правительства РФ от 26.06.1995 О сертификации средств защиты информации N 608
- Постановление Правительства РФ от 15 августа 2006 г. N 504 О лицензировании деятельности по технической защите конфиденциальной информации
- Постановление Правительства РФ от 31 августа 2006 г. N 532 О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации
- Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"
- Постановление Правительства Российской Федерации от 17 ноября 2007 г. N 781 г. Москва "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"
- Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне»

Международные стандарты в области ИБ:

- BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров мирового

опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ

- BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.
- BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности
- ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.
- ISO/IEC 27000 — Словарь и определения.
- ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
- ISO/IEC 27002 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.
- ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
- ISO/IEC 31000 — Описание подхода к риск-менеджменту без привязки к ИТ/ИБ.
- German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

История криптографии и шифрования

Самым древним свидетельством применения шифра (около 4000 до н.э.) ученые считают древнеегипетский папирус с перечислением монументов времен фараона Аменемхета II.

В IV столетии до н.э. автор военных трактатов Эней Тактик придумал шифровальный диск, названный впоследствии его именем. Для записи сообщения в отверстия диска с подписанными рядом с ними буквами последовательно продевалась нить. Чтобы прочитать текст, нужно было всего лишь вытягивать нить в обратной последовательности. Это и составляло основной минус устройства – при наличии времени шифр мог быть разгадан любым грамотным человеком. Зато, чтобы быстро «стереть» информацию с диска Энея, нужно было всего лишь вытянуть нить или разбить устройство.

Одним из первых документально зафиксированных шифров является шифр Цезаря (около 100 г. до н.э.). Его принцип был очень прост: каждая буква исходного текста заменялась на другую, отстоящую от нее по алфавиту на определенное число позиций. Зная это число, можно был разгадать шифр и узнать, какие тайны Цезарь передавал своим генералам.

Интересно, что в Древней Руси тоже были свои способы тайнописи, например, литорея, которая делилась на простую и мудрую. В мудрой версии шифра некоторые буквы заменялись точками, палками или кругами. В простой литорее, которая еще называлась тарабарской грамотой, все согласные буквы кириллицы располагались в два ряда. Зашифровывали письмо, заменяя буквы одного ряда буквами другого (рис. 1).

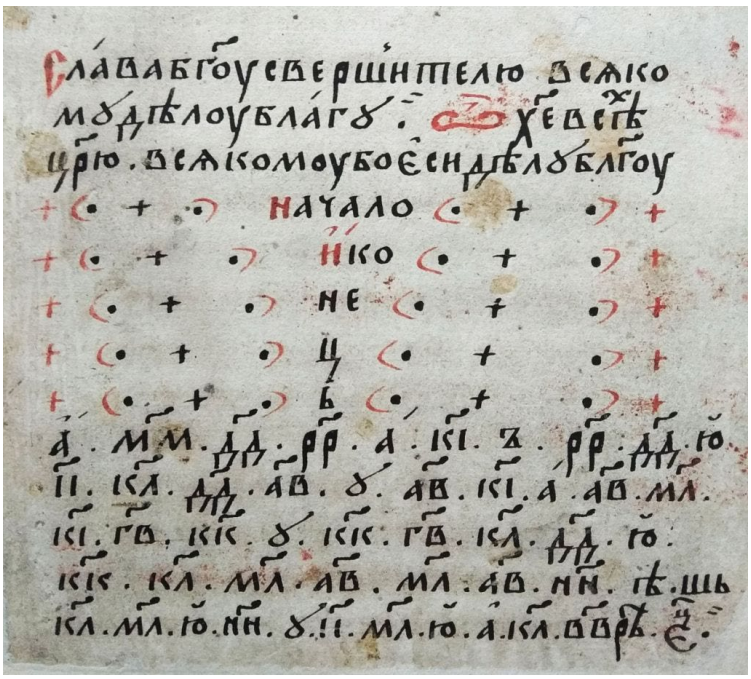

Рис.1

Около 1466 года итальянский ученый Леон Альберти изобретает шифровальный диск (рис. 2), состоящий из двух частей: внешней и внутренней. На неподвижном внешнем диске был написан алфавит и цифры. Внутренний подвижный диск также содержал буквы и цифры в другом порядке и являлся ключом к шифру. Для шифрования нужно было найти нужную букву текста на внешнем диске и заменить ее на букву на внутреннем,

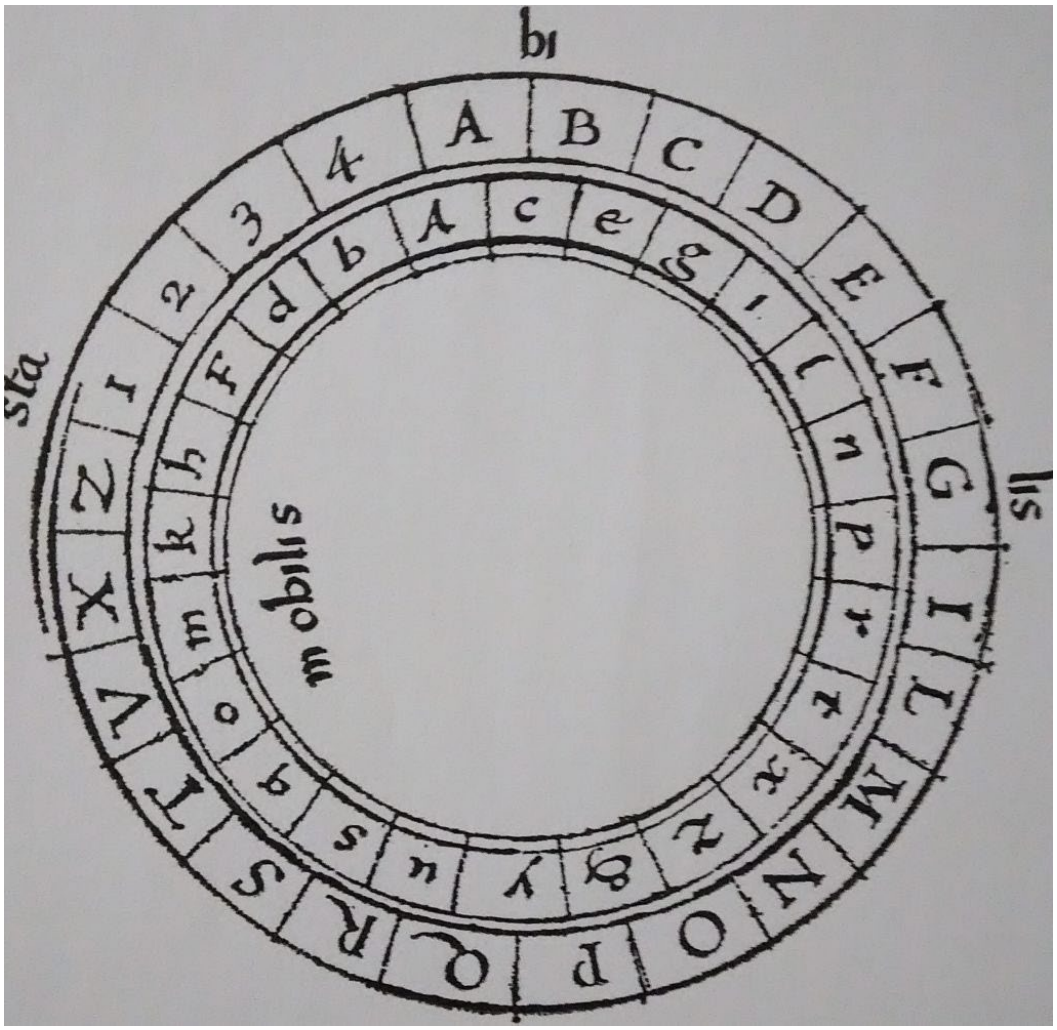

Рис.2

стоящую под ней. После этого внутренний диск сдвигался, и новая буква зашифровывалась уже с новой позиции. Таким образом, шифр Альберти стал одним из первых шифров многоалфавитной замены, основанных на принципе комбинаторики. Кроме того, Леон Альберти написал одну из первых научных работ по криптографии − «Трактат о шифрах».

Посол Франции в Риме Блез де Виженер, познакомившись с трудами Тритемия, Белазо, Кардано, Порта, Альберти в области криптографии также увлекся ею. В 1585 году он написал «Трактат о шифрах», в котором излагаются основы криптографии. В этом труде он замечает: «Все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом». Эта мысль была позднее повторена Блезом Паскалем — одним из основоположников теории вероятностей, а в XX веке и Норбертом Винером — «отцом кибернетики».

Виженер объединил подходы Тритемия, Беллазо, Порта к шифрованию открытых текстов, по существу, не внеся в них ничего оригинального. В наше время «шифр Виженера», состоящий в периодическом продолжении ключевого слова по таблице Тритемия, вытеснил имена его предшественников.

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр» англ. *The Alphabet Cipher*, опубликованной в детском журнале в 1868 году. В 1917 году Scientific American также отозвался о шифре Виженера как о не поддающемся взлому.

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски. Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе Гражданской войны. Послания Конфедерации были далеки от секретных, и их противники регулярно взламывали сообщения. В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например, в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря

Во Второй мировой войне противники уже использовали мобильные электромеханические шифраторы, шифры которых считались не раскрываемыми. Устройства были роторными или на цевочных дисках. К первым относилась знаменитая машина «Энигма», которой пользовались нацисты, ко вторым – американская машина М-209.

Принцип работы «Энигмы» заключался в следующем: при каждом нажатии на клавишу с буквой алфавита в движение приходили один или несколько роторов. Буква изменялась несколько раз по принципу шифра Цезаря, и в окошке выдавался результат. Шифры «Энигмы» считались самыми стойкими для взлома, так как количество ее комбинаций достигало 15 квадриллионов. Однако код «Энигмы» все же был расшифрован, сперва польскими криптографами в 1932 году, а затем английским ученым Аланом Тьюрингом, создавшим машину для расшифровки сообщений «Энигмы» под названием «Бомба». Комплекс из 210 таких машин позволял англичанам расшифровывать до 3 тыс. военных сообщений нацистов в сутки и внес большой вклад в победу союзников.

Обсуждение опыта проведения уроков безопасного Интернета

Кроме борьбы с негативным контентом, важнейшей задачей молодежной кибердружины является ***просветительская деятельность, проводимая среди учащихся школ***, и создание нового позитивного контента. В рамках своей работы участники кибердружин занимаются повышением уровня компьютерной грамотности учащихся и дают им основы знаний в сфере информационной безопасности.

Информационные войны ведутся уже много веков, но именно развитие сети Интернет привело к значительному росту опасности данного вида противостояния – появлению информационного оружия, основанного на использование применении ИКТ. Усиление информационной агрессии в отношении нашего государства является серьезной угрозой национальной безопасности. Примерами такой агрессии становятся информационные сообщения на Интернет-форумах, блогах, в социальных сетях, статьи в сетевых СМИ, комментарии к подобным статьям.

Оружием информационных войн, к сожалению, все чаще становятся поисковые системы в сети Интернет. Сообщения антигосударственной направленности со временем выводятся поисковой системой на все более высокие позиции в ответ на определенные запросы пользователей. Создается впечатление, что наиболее авторитетные источники поддерживают точку зрения автора, ведущего информационную войну.

Для противостояния информационной агрессии участникам казачьей кибердружины требуется четко понимать механизмы ведения информационной войны.

Создание позитивной и полезной информации в сети Интернет. Огромную важность приобретает создание действительно качественного контента, его предоставление в той форме, которая наилучшим образом воспринимается аудиторией сети Интернет. К нему может быть отнесено создание молодежных СМИ, групп в социальных сетях и каналов на видеохостинговых сервисах (таких как «Youtube» и «Rutube»). Размещение кибердружинниками качественно оформленного и смонтированного контента, направленного на сохранение культуры, духовных ценностей и национальной идентичности, позволит создать тот защитный рубеж, который так нужен сейчас нашей стране в условиях усиливающейся информационной агрессии.

Правоохранительным органам с каждым годом все сложнее отслеживать стремительно растущие объемы информации противоправной и запрещенной направленности, акты информационной агрессии, деятельность преступных и экстремистских сообществ в сети Интернет. Именно кадет обучению принципам противостояния киберугрозам может стать одной из важных основ будущей доктрины национальной безопасности. Развитие молодежных кибердружин способно сделать их грозным оружием в борьбе с киберпреступностью и информационной агрессией в сети Интернет. Структура работы молодежной кибердружины на базе образовательной организации представлена на рис. 2.

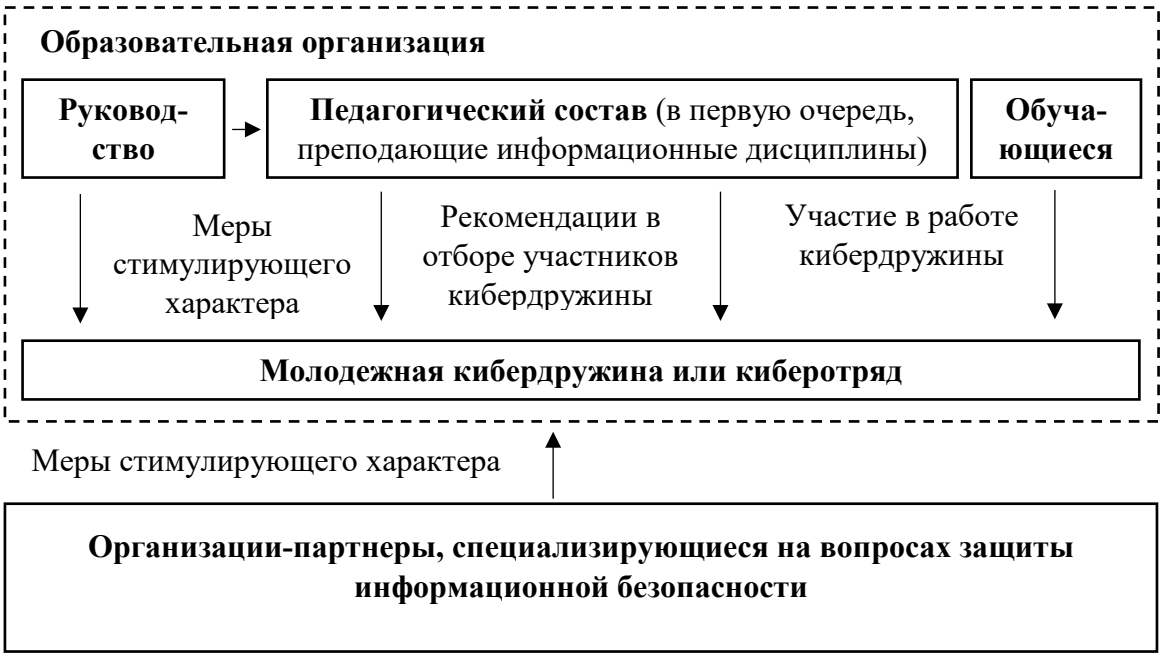

Рис 2. Модель функционирования молодежной кибердружины (киберотряда) на базе образовательной организации.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ «ИНТЕРНЕТ». «БОЛЬШИЕ ДАННЫЕ»

Защита персональных данных в сети «Интернет».

Персональные данные - это фамилия, имя, отчество, дата и место рождения, адрес, семейное положение, паспортные данные, профессия, место работы, доходы и другая информация, с помощью которой может быть определена личность пользователя. Не являются персональными данными пароли к аккаунтам, так как они не сообщают никакой информации о человеке.

Обработка персональных данных должна осуществляться с согласия субъекта персональных данных на их обработку. Персональные данные являются конфиденциальными, но с согласия их владельца они могут становиться общедоступными (номер телефона, e-mail), так же, как и по его требованию они должны быть убраны из общего доступа. Обеспечение конфиденциальности персональных данных не требуется в случае их обезличивания.

В интернете персональные данные могут потребоваться при регистрации электронной почты, в различных социальных сетях, при пользовании услугами электронной коммерции, персонифицированными государственными услугами (on-line подача заявления на регистрацию транспортного средства), интернет – рекрутинг (размещение резюме на сайтах поиска работы).

Такое использование личных данных как их размещение на корпоративных сайтах компании осуществляется с согласия их владельца.

Поэтому и вопрос об информационной безопасности личных данных в современном мире является очень актуальным. С развитием информационных технологий укрепилась и правовая база, регулирующая деятельность в сфере обработки персональных данных.

В Российской Федерации защита персональных данных граждан, в том числе и при обработке персональных данных с использованием средств автоматизации, основана на Конституции РФ, международных договорах РФ, Федеральном законе № 152 – ФЗ от 27.07.2006 «О персональных данных» и других законодательных и нормативно-правовых актах.

Защита персональных данных должна обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных, право на неприкосновенность частной жизни, личной и семейной тайны, конфиденциальность предоставляемой информации, а также не допущение

уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также предотвращение случайного доступа к ним и других неправомерных действий.

Комплекс мер по защите персональных данных включает в себя использование шифровальных средств, антивирусной защиты, защиты доступа к информации индивидуальным паролем, анализ защищенности, обнаружение и предотвращение вторжений, управление доступом, регистрацию и учет[1].

Определение понятия «больших данных».

К категории Большие данные (Big Data) относится информация, которую уже невозможно обрабатывать традиционными способами, в том числе структурированные данные, медиа и случайные объекты. Некоторые эксперты считают, что для работы с ними на смену традиционным монолитным системам пришли новые массивно-параллельные решения.

Изначально с большими данными связывали три ключевых концепции (правило «трех V»):

Объем (volume). Данные в компании накапливаются из множества источников в громадном объеме.

Скорость роста (velocity). Быстрое возрастание объемов данных. Особенно характерно для компаний в области сетевой торговли и электронной коммерции, где ежедневно могут генерироваться сотни терабайт данных.

Многообразие (variety). Данные из входного потока могут быть разнообразных форматов (таблицы, текст, видео, аудио и пр.), а также быть структурированными и неструктурированными.

Постепенно правило «трех V» обогатилось дополнительными элементами и трансформировалось в: «четыре V» (veracity — достоверность), «пять V» (viability — жизнеспособность и value — ценность) и «семь V» (variability — переменчивость и visualization — визуализация).

В настоящее время понятие «большие данные» связано с использованием предсказательной и поведенческой аналитики и других направлений анализа данных с целью извлечения знаний из огромных массивов данных.

Главными проблемами, с которыми приходится сталкиваться при работе с большими данными, являются возрастание вычислительных затрат — как в

[1] Жигайло В.А. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ // Научное сообщество студентов: МЕЖДИСЦИПЛИНАРНЫЕ ИССЛЕДОВАНИЯ: сб. ст. по мат. XXXVII междунар. студ. науч.-практ. конф. № 2(37). URL: https://sibac.info/archive/meghdis/2(37).pdf (дата обращения: 01.02.2020)

плане времени, так и требуемых объемов памяти. Отсюда вытекают задачи оптимизации размещения данных в оперативной памяти, количества обращений к диску и числа проходов по данным.

Принципы автоматизации процесса поиска противоправного Интернет-контента.

Так, например, компания «Мегапьютер Интеллидженс», один из отечественных лидеров в сфере анализа данных, предоставляет образовательным организациям доступ к своему продукту «PolyAnalyst».

Предоставление участникам молодежных кибердружин (киберотрядов) системы «PolyAnalyst», ведущего российского программного обеспечения в сфере извлечения полезной информации из структурированных и неструктурированных данных, и освоение кибердружиниками функционала данного программного комплекса позволит обучающимся кадетских классов включиться в работу «Роскомнадзора» по автоматизации поиска противоправного контента.

КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА КИБЕРПРОСТРАНСТВА

Кибербезопасность – что это такое

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации)

Способы несанкционированного доступа (НСД) как проблему утечки конфиденциальной информации предлагается рассматривать со следующих позиций. Вопрос обеспечения защиты от НСД связан с проблемой сохранности не только информации как вида интеллектуальной собственности, но физических и юридических лиц, их имущественной собственности и личной безопасности. Известно, что такая деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Как только информация представляет определенную цену, факт ее получения злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Отсюда главная цель противоправных действий – получение информации о составе, состоянии и деятельности объекта конфиденциальной информации для удовлетворения своих информационных потребностей в корыстных целях и внесение изменений в состав информации. Такое действие может привести к дезинформации в определенных сферах деятельности и отражаться, в частности, на учетных данных, результатах решения управленческих задач[2].

Утечку информации можно рассматривать как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена. При этом природа утечки охраняемой информации характеризуется как обстоятельствами происхождения, так и причинами, условиями возникновения утечки[3].

Кибертерроризм и кибервойны

Теоретически доказано, а практикой многократно подтверждено то, что психика и мышление человека подвержены внешним информационным воздействиям и при их надлежащей организации возникает возможность

[2] Артемов А.В. Информационная безопасность. Курс лекций - М.: Академия безопасности и выживания, 2014. — 161 с. – с. 13

[3] Артемов А.В. Информационная безопасность. Курс лекций - М.: Академия безопасности и выживания, 2014. — 161 с. – с. 11

программирования поведения человека. Более того, в последнее время ведутся разработки методов и средств компьютерного проникновения в подсознание, для того чтобы оказывать на него глубокое воздействие. Поэтому актуальной является проблема не только защиты информации, но и защиты от разрушающего воздействия информации, приобретающей международный масштаб и стратегический характер. В силу изменения концепции развития стратегических вооружений, определяющей, что вооруженное решение мировых проблем становится невозможным, все более прочно входит в обиход понятие ***информационной войны*** . Сейчас эффективность наступательных средств информационной войны, информационного оружия превосходит эффективность систем защиты информации[4].

Хакерские атаки. Виды атак

Угроза – это потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба

Уязвимость – это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Атака – это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.

Из определений видно, что, производя атаку, нарушитель использует уязвимости информационной системы. Иначе говоря, если нет уязвимости, то невозможна и атака, её использующая. Поэтому одним из важнейших механизмов защиты является процесс поиска и устранения уязвимостей информационной системы. Рассмотрим различные классификации уязвимостей. Часть уязвимостей закладывается ещё на этапе проектирования. Другая часть уязвимостей возникает на этапе реализации (программирования). И, наконец, уязвимости могут быть следствием ошибок, допущенных в процессе эксплуатации информационной системы. Сюда относятся неверное конфигурирование операционных систем, протоколов и служб, нестойкие пароли пользователей и др.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Одни атаки отличаются большой сложностью, другие может

[4] Артемов А.В. Информационная безопасность. Курс лекций - М.: Академия безопасности и выживания, 2014. — 161 с. – с. 10

осуществить обычный оператор, даже не предполагающий, какие последствия будет иметь его деятельность.

Наиболее распространены следующие атаки.

Подслушивание. В основном данные по компьютерным сетям передаются в незащищенном формате (открытом тексте), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в сети подслушивать и считывать трафик.

Изменение данных. Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг – изменить их. Данные в пакете могут быть изменены, даже если злоумышленник ничего не знает ни об отправителе, ни о получателе.

Анализ сетевого трафика. Целью атак подобного типа является прослушивание каналов связи и анализ передаваемых данных и служебной информации для изучения топологии и архитектуры построения системы, получения критической пользовательской информации (например, паролей пользователей или номеров кредитных карт, передаваемых в открытом виде).

Подмена доверенного субъекта. Большая часть сетей и ОС используют IP-адрес компьютера для того, чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом). Такой способ атаки называют фальсификацией адреса.

Посредничество. Эта атака подразумевает активное подслушивание, перехват и управление передаваемыми данными невидимым промежуточным узлом. Когда компьютеры взаимодействуют на низких сетевых уровнях, они не всегда могут определять, с кем именно они обмениваются данными.

Перехват сеанса. По окончании начальной процедуры аутентификации соединение, установленное законным пользователем, например, с почтовым сервером, переключается злоумышленником на новый хост, а исходному серверу выдается команда разорвать соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным.

Отказ в обслуживании (Denial of Service, DoS). Эта атака отличается от атак других типов: она не нацелена на получение доступа к сети или на получение из этой сети какой-либо информации. Атака DoS делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, ОС или приложения. По существу, она лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Парольные атаки. Их цель – завладение паролем и логином законного пользователя. Часто хакеры пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой метод носит название атака полного перебора (brute force attack). Для этой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате злоумышленнику удается подобрать пароль, он получает доступ к ресурсам на правах обычного пользователя.

Парольных атак можно избежать, если не пользоваться паролем в текстовой форме. Использование одноразовых паролей и криптографической аутентификации может практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные методы аутентификации.

При использовании обычных паролей необходимо придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее 8 символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, $, &, % и т.д.).

Угадывание ключа. Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа не просто и требует больших затрат ресурсов, тем не менее это возможно. В частности, для определения значения ключа может быть использована специальная программа, реализующая метод полного перебора. Ключ, к которому получает доступ атакующий, называется скомпроментированным. Атакующий использует скомпроментированный ключ для получения доступа к защищенным передаваемым данным без ведома отправителя и получателя. Ключ дает возможность расшифровывать и изменять данные.

Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации[5].

[5] Соловьев А.А., Метелев С.Е., Зырянова С.А. Защита информации и информационная безопасность - Учебник. — Омск: Изд-во Омского института (филиала) РГТЭУ, 2011. – 426 с. – с. 114

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ УСТРОЙСТВ

Борьба с утечками информации

Средства контроля доступа и права пользователей.

Контроль доступа – это способ защиты информации от несанкционированного доступа путем регулирования прав пользователей на использование тех или иных ресурсов автоматизированной системы. Необходимость контроля доступа возникает при использовании общего ресурса многими пользователями. В компьютерных сетях, где информация хранится, обрабатывается и передается файлами (либо частями файлов), доступ к информации регламентируется на уровне файлов (*объектов доступа*). Сложнее организуется доступ в базах данных, в которых он может регламентироваться к отдельным ее частям по определенным правилам.

При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять тому или иному пользователю (*субъекту доступа*).

Различают следующие операции с файлами:

- чтение (R);
- запись;
- выполнение программ (E).

Операция записи в файл имеет две модификации. Субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла (W). Другая организация доступа предполагает разрешение только дописывания в файл, без изменения старого содержимого (A)[6].

Подсистема защиты данных является одной из наиболее важных. В центре системы безопасности, например, в операционной системе Windows находится система контроля доступа.

С каждым процессом или потоком, то есть активным компонентом (**субъектом**), связан маркер доступа, а у каждого защищаемого объекта (например, файла) имеется дескриптор защиты. Проверка прав доступа обычно осуществляется в момент открытия объекта и заключается в сопоставлении прав **субъекта** списку прав доступа, который хранится в составе дескриптора защиты **объекта**

[6] Аникин Д.В. Информационная безопасность и защита информации - СПб.: Институт электронного обучения Санкт-Петербургского университета технологий управления и экономики, 2011. — 269 с. – с. 48-49

Помимо дискреционного доступа Windows поддерживает управление **привилегированным доступом**. Это означает, что в системе имеется пользователь-администратор с неограниченными правами.

Кроме того, для упрощения администрирования пользователи Windows объединены в **группы**. Пользователь, как член группы, облекается, таким образом, набором полномочий, необходимых для его деятельности, и играет определенную роль. Подобная стратегия называется **управление ролевым доступом**.

Ключевая цель системы защиты Windows - следить за тем, кто и к каким объектам осуществляет доступ. Система защиты хранит информацию, относящуюся к безопасности для каждого пользователя, группы пользователей и объекта. Модель защиты в Windows требует, чтобы субъект на этапе открытия объекта указывал, какие операции он собирается выполнять в отношении этого объекта[7].

Способы разграничения доступа.

В области многоуровневых систем разграничения доступа преобладающей идеей, в течение последнего десятилетия определявшей основное направление исследований, является концепция разработки защищенной универсальной операционной системы на базе так называемого ядра безопасности. Под ядром безопасности понимают локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, реализующих функции диспетчера доступа и ряд других сопутствующих служебных функций.

К аппаратным средствам поддержки защиты и изоляции ядра безопасности относятся:

- многоуровневые, привилегированные режимы выполнения команд (с числом уровней больше двух);
- использование ключей защиты и сегментирование памяти; – реализация механизма виртуальной памяти с разделением адресных пространств;
- аппаратная реализация функций ОС;
- хранение и распространение программ в ПЗУ;
- использование новых архитектур ЭВМ (с отходом от фоннеймановской архитектуры в сторону повышения структурной сложности

[7] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 283

базовых машинных объектов – архитектуры с реализацией абстрактных типов данных, теговые архитектуры с привилегиями и т. п.).

Шифрование, цифровая подпись и политика безопасности

Криптография – тайнопись, система разнообразных способов изменения формы отображения информации (текста, речи), позволяющих сделать содержание информации непонятным для лиц, не владеющих знанием использованного шифра. Криптографические методы представляют собой *шифрование,* кодирование, сжатие, расчленение (разнесение) информации. Криптография входит составной частью в понятие криптологии, в которое включается также криптоанализ – дешифрование текста или речи известным ключом или без него.

Шифрование – криптографическое (математическое, алгоритмическое) преобразование информации с целью получения шифрованного текста или устной речи (см. также *Криптография).*

Что такое цифровая подпись.

Цифровые подписи - это форма шифрования, обеспечивающая аутентификацию (подтверждение подлинности) цифровой информации.

С помощью цифровой подписи можно повысить уровень этой защиты и обезопасить информацию от изменения после получения и дешифрования.

До настоящего времени наиболее часто для построения схемы цифровой подписи использовался алгоритм RSA. В основе этого алгоритма лежит концепция Диффи-Хеллмана. Она заключается в том, что каждый пользователь сети имеет свой закрытый ключ, необходимый для формирования подписи; соответствующий этому секретному ключу открытый ключ, предназначенный для проверки подписи, известен всем другим пользователям сети[8].

Первый отечественный стандарт ЭЦП появился в 1994 году. Вопросами использования ЭЦП в России занимается Федеральное агентство по информационным технологиям (ФАИТ)[9].

[8] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 251

[9] Соловьев А.А., Метелев С.Е., Зырянова С.А. Защита информации и информационная безопасность - Учебник. — Омск: Изд-во Омского института (филиала) РГТЭУ, 2011. – 426 с. – с. 18

Проблемы безопасности информационных систем в различных сферах деятельности

Основные направления обеспечения информационной безопасности компьютерных сетей образовательных организаций.

В настоящее время противоречие между требованиями к защите ресурсов компьютерных сетей учебных заведений и ростом компьютерных преступлений определяет одну из важных задач – построение интегрированной системы безопасности образовательных организаций. Данная проблема включает в себя комплексное решение задач определения нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации в процессе обучения. Несмотря на видимую схожесть задач защиты корпоративных сетей и компьютерных сетей образовательных организаций, задача по обеспечению безопасности их сетей не получила окончательного решения.

Кроме общих проблем внедрения технологий безопасности для сетей образовательных организаций можно отметить две специфические:

- отсутствие единой технической политики информационной безопасности в области образования;
- в образовательных организациях, как известно, сосредоточены наиболее вероятные потенциальные нарушители безопасности компьютерных систем[10].

Проблемы безопасности банковских систем.

В наши дни в связи со всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возросло. Еще 30 лет назад объектом информационных атак были данные о клиентах банков или о деятельности самого банка. Такие атаки были редкими, круг их заказчиков был очень узок, а ущерб мог быть значительным лишь в особых случаях. В настоящее время в результате повсеместного распространения электронных платежей, пластиковых карт, компьютерных сетей объектом информационных атак стали непосредственно денежные средства как банков, так и их клиентов. Совершить попытку хищения может

[10] Артемов А.В. Информационная безопасность. Курс лекций - М.: Академия безопасности и выживания, 2014. — 161 с. – с. 101

любой – необходимо лишь наличие компьютера, подключенного к сети Интернет. Причем для этого не требуется физически проникать в банк, можно «работать» и за тысячи километров от него ***безопасность платежных систем.***

В западных банках программное обеспечение (ПО) разрабатываются конкретно под каждый банк и устройство информационной системы во многом является коммерческой тайной. В России получили распространение «стандартные» банковские пакеты, информация о которых широко известна, что облегчает несанкционированный доступ в банковские компьютерные системы. Причем, во-первых, надежность «стандартного» ПО ниже из-за того разработчик не всегда хорошо представляет конкретные условия, в которых этому ПО придется работать, а во-вторых, некоторые российские банковские пакеты не удовлетворяли условиям безопасности.

Чаще всего происходят не такие нарушения, как нападения хакеров или кража компьютеров с ценной информацией, а самые обыкновенные, проистекающие из повседневной деятельности. В то же время именно умышленные атаки на компьютерные системы приносят наибольший единовременный ущерб, а меры защиты от них наиболее сложны и дорогостоящи. В этой связи проблема оптимизации защиты информационных систем является наиболее актуальной в сфере информационной безопасности банков[11].

[11] Артемов А.В. Информационная безопасность. Курс лекций - М.: Академия безопасности и выживания, 2014. — 161 с. – с. 55-57

ВИРУСЫ И АНТИВИРУСЫ

Вирусное программное обеспечение и иные киберугрозы

Типы и разновидности вирусов.

Компьютерный вирус - это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Условно жизненный цикл любого компьютерного вируса можно разделить на пять стадий:

- Проникновение на чужой компьютер.
- Активация.
- Поиск объектов для заражения.
- Подготовка копий.
- Внедрение копий[12].

Абсолютно надёжных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Только многоуровневая оборона способна обеспечить наиболее полную защиту от вирусов. Важным элементом защиты от компьютерных вирусов является профилактика. Антивирусные программы применяют одновременно с регулярным резервированием данных и профилактическими мероприятиями. Вместе эти меры позволяют значительно снизить вероятность заражения вирусом.

Основными мерами профилактики вирусов являются:

1) применение лицензионного программного обеспечения;

2) регулярное использование нескольких постоянно обновляемых антивирусных программ для проверки не только собственных носителей информации при переносе на них сторонних файлов, но и любых «чужих» дискет и дисков с любой информацией на них, в т.ч. и переформатированных;

3) применение различных защитных средств при работе на компьютере в любой информационной среде (например, в Интернете). Проверка на наличие вирусов файлов, полученных по сети;

[12] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 160

4) периодическое резервное копирование наиболее ценных данных и программ[13].

Выявление неизвестных вирусов.

О наличии вируса в автоматизированной системе пользователь может судить по следующим событиям: появление сообщений антивирусных средств о заражении или о предполагаемом заражении; явные проявления присутствия вируса, такие как сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в автоматизированной системе; неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств автоматизированной системы.

К неявным проявлениям наличия вирусов в автоматизированной системе можно отнести «зависания» системы, замедление выполнения определенных действий, нарушение адресации, сбои устройств и тому подобное[14].

Признаки и диагностика заражений через браузер. Явные проявления обычно заражений через Браузер выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие проникновения на компьютер рекламной утилиты. Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также явные проявления могут вызывать ряд троянских программ, например, утилиты несанкционированного дозвона к платным сервисам. Они вынуждены быть явными, поскольку используемые ими приложения сложно использовать незаметно от пользователя.

Подозрительные процессы. Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов (в ОС семейства Windows вызывается через CTRL+ALT+DEL) подозрительных программ. Исследуя этот список и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, то есть до начала работы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих лишь только скрытые или косвенные проявления.

---

[13] Соловьев А.А., Метелев С.Е., Зырянова С.А. Защита информации и информационная безопасность - Учебник. — Омск: Изд-во Омского института (филиала) РГТЭУ, 2011. – 426 с. – с. 16

[14] Аникин Д.В. Информационная безопасность и защита информации - СПб.: Институт электронного обучения Санкт-Петербургского университета технологий управления и экономики, 2011. — 269 с. – с. 154

Сетевая активность. Неожиданно возросшая сетевая активность может служить ярким свидетельством работы на компьютере подозрительный программы. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, например, для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

Изучить и проанализировать сетевую активность можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно устанавливаемыми приложениями. В этом задании это предлагается сделать с помощью Диспетчера задач Windows.

Элементы автозапуска. Для того, чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили. Оптимальным с точки зрения вируса вариантом служит запуск одновременно с операционной системой - в этом случае запуск практически гарантирован.

Вредоносная программа может вносить изменения в системные файлы win.ini и system.ini[15].

Черви, трояны и скрипты

По механизму распространения различают:

- **вирусы** - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- **«черви»** - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. «Черви», напротив, ориентированы в первую очередь на распространение по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, «черви» «съедают» полосу пропускания сети и ресурсы почтовых

[15] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 183

систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных «бомб».

Вредоносный код, который выглядит как функционально полезная программа, называется **троянским вирусом**. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке[16].

Троян (троянский конь) - программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы, с целью проникновения в нее. Однако в большинстве случаев они проникают на компьютеры вместе с вирусом либо червем - то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу. Нередко пользователи сами загружают троянские программы из Интернет[17].

Поскольку главная цель написания троянов - это производство несанкционированных действий, они классифицируются по типу вредоносной нагрузки.

1. Клавиатурные шпионы, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.

2. Похитители паролей предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.

3. Утилиты скрытого удаленного управления - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Перечень действий, которые позволяет выполнять тот или иной троян, определяется его функциональностью, заложенной автором. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как

[16] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 55

[17] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 164

для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных.

4. Люки (backdoor) — трояны предоставляющие злоумышленнику ограниченный контроль над компьютером пользователя. От утилит удаленного управления отличаются более простым устройством и, как следствие, небольшим количеством доступных действий. Тем не менее, обычно одними из действий являются возможность загрузки и запуска любых файлов по команде злоумышленника, что позволяет при необходимости превратить ограниченный контроль в полный.

5. Анонимные сервера - разновидность троянов, которые на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.

6. Утилиты дозвона - в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.

7. Модификаторы настроек браузера меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.

8. Логические бомбы характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов.

Скрипт-вирусы, написанные в виде скриптов для определенной командной оболочки - например, bat-файлы для DOS или VBS и JS - скрипты для Windows Scripting Host (WSH)[18].

Хакерские утилиты

Хакерские утилиты - К этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.

[18] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 160

Антивирусная защита ПК, сети и мобильных пользователей

Антивирусные программы.

Антивирус - программное средство, предназначенное для борьбы с вирусами.

Основными задачами антивируса является:

- Препятствование проникновению вирусов в компьютерную систему.
- Обнаружение наличия вирусов в компьютерной системе.
- Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы.
- Минимизация ущерба от действий вирусов.

Помимо используемых технологий, антивирусы отличаются друг от друга условиями эксплуатации. Уже из анализа задач можно сделать вывод о том, что препятствование проникновению вредоносного кода должно осуществляться непрерывно, тогда как обнаружение вредоносного кода в существующей системе - скорее разовое мероприятие. Следовательно, средства, решающие эти две задачи должны функционировать по-разному.

Таким образом, антивирусы можно разделить на две большие категории:

- **Предназначенные для непрерывной работы** - к этой категории относятся средства проверки при доступе, почтовые фильтры, системы сканирования проходящего трафика Интернет, другие средства, сканирующие потоки данных.
- **Предназначенные для периодического запуска** - различного рода средства проверки по запросу, предназначенные для однократного сканирования определенных объектов. К таким средствам можно отнести сканер по требованию файловой системы в антивирусном комплексе для рабочей станции, сканер по требованию почтовых ящиков и общих папок в антивирусном комплексе для почтовой системы[19].

Антивирусные программы для ПК: сканеры, ревизоры и др.

Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации, образуя методы борьбы с вирусами. Можно выделить методы обнаружения вирусов и методы удаления вирусов.

[19] Макаренко С.И. Информационная безопасность - Учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. – с. 183-185

Сканирование – один из самых простых методов обнаружения вирусов. Сканирование осуществляется программой-сканером, которая просматривает файлы в поисках **сигнатуры** – совокупности черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Совокупность сигнатур известных вирусов составляют антивирусную базу программы-сканера.

Задачу выделения сигнатур, как правило, решают люди – эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. В наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур. Например, в случае несложных по структуре троянских коней или червей, которые не заражают другие программы, а целиком являются вредоносными программами.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вирусов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются. Тем не менее, между антивирусными компаниями существует договоренность об обмене образцами вирусов, а значит рано или поздно сигнатура нового вируса попадает в антивирусные базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех. Одно из распространенных заблуждений насчет сигнатур заключается в том, каждая сигнатура соответствует ровно одному вирусу или вредоносной программе. А потому антивирусная база с большим количеством сигнатур позволяет обнаруживать больше вирусов. На самом деле это не так. Очень часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому считать, что количество сигнатур равно количеству обнаруживаемых вирусов, уже нельзя. Соотношение количества сигнатур и количества известных вирусов для каждой антивирусной базы свое и вполне может оказаться, что база с меньшим количеством сигнатур в действительности содержит информацию о большем количестве вирусов. Если же вспомнить, что антивирусные компании обмениваются образцами вирусов, можно с высокой долей уверенности считать, что антивирусные базы наиболее известных антивирусов *эквивалентны*.

Важное дополнительное свойство сигнатур – точное и гарантированное определение типа вируса. Это свойство позволяет занести в базу не только

сами сигнатуры, но и способы лечения вируса. Если бы сигнатурный анализ давал только ответ на вопрос, есть вирус или нет, но не давал ответа, что это за вирус, то лечение инфицированного файла было бы невозможно - слишком большим был бы риск совершить не те действия и вместо лечения получить дополнительные потери информации.

Другое важное, но уже отрицательное свойство – для получения сигнатуры необходимо иметь образец вируса. Следовательно, сигнатурный метод непригоден для защиты от новых вирусов, т. к. до тех пор, пока вирус не попал на анализ к экспертам, создать его сигнатуру невозможно. Именно поэтому все наиболее крупные эпидемии вызываются новыми вирусами. С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры почти беспрепятственно.

Метод обнаружения изменений базируется на использовании программ **ревизоров**. Эти программы определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы. При периодическом выполнении программ-ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков. По результатам ревизии программа выдает сведения о предположительном наличии вирусов. Обычно программы-ревизоры запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, характеристики всех контролируемых файлов, каталогов и номера дефектных кластеров. Могут контролироваться также объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры.

Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов. Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему *уже зараженными*. Вирусы будут обнаружены только после размножения в системе[20].

Межсетевые экраны.

Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением

[20] Аникин Д.В. Информационная безопасность и защита информации - СПб.: Институт электронного обучения Санкт-Петербургского университета технологий управления и экономики, 2011. — 269 с. – с. 144-145

разрешенных данных. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки.

Межсетевые экраны, представляют собой программные пакеты, базирующиеся на операционных системах общего назначения (таких как Windows NT и Unix) или на аппаратной платформе межсетевых экранов. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты. Правила политики безопасности усиливаются посредством использования модулей доступа.

КИБЕРПРЕСТУПЛЕНИЯ. ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ КИБЕРПРОСТРАНСТВА

Собственность в Интернете и защита прав потребителей при использовании услуг Интернет. Ответственность за киберпреступления и интернет-мошенничество

Авторское право.

Заявление авторских прав на программное обеспечение (ПО) применяется в качестве наиболее общего способа защиты ПО. Обладание авторским правом на ПО относит практически все операции по манипулированию этим ПО (продажа, применение, развитие) в исключительное ведение владельца.

Вместе с тем применение Закона об авторских правах для защиты ПО сталкивается с некоторыми проблемами, в частности с проблемой создания ПО в рамкам служебного задания.

Другой проблемой применения этого Закона для защиты ПО является вопрос о границах действия охраны прав на ПО – охраняется ли алгоритм,

текст и структура программы или внешний способ организации взаимодействия с пользователем[21].

Как расследуются преступления в сети.

Анализ практики борьбы с преступностью на современном этапе развития общества дает основание считать, одним из распространенных видов киберпреступлений является неправомерный доступ к информации в компьютерных сетях.

В ст. 272 УК РФ дается перечень последствий такого преступления. К ним относятся: модификация, уничтожение, блокирование или копирование информации либо нарушение работы ЭВМ, системы ЭВМ или их сети.

Установить виновность и мотивы неправомерного доступа к компьютерной информации можно только по совокупности результатов всех процессуальных действий. Решающими из них являются допросы свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных аппаратно-компьютерных и программно-компьютерных экспертиз, а также результаты обыска.

В процессе их производства выясняется: во-первых, с какой целью совершен несанкционированный доступ к компьютерной информации; во-вторых, знал ли правонарушитель о существующей системе ее защиты; в-третьих, желал ли он преодолеть эту систему; в-четвертых, если желал, то какие конкретно для этого им приняты меры[22]

Кибернаемники и кибердетективы.

Следует рассмотреть практическую деятельность специальных подразделений МВД по борьбе с преступлениями в сфере высоких технологий (подразделений «К»), которая сосредоточена на следующих направлениях:

- преступления в сфере компьютерной информации и телекоммуникационных сетях;
- незаконный оборот объектов интеллектуальной собственности на электронных носителях;
- незаконный оборот электронных систем и специальных технических средств;

---

[21] Артемов А.В. Информационная безопасность. Курс лекций - М.: Академия безопасности и выживания, 2014. — 161 с. – с. 114

[22] Авсентьев О.С., Немцова А.А., Скрыль С.В., Скрыль К.С., Филиппова Н.В. Методические основы выявления и предупреждения преступных посягательств на компьютерную информацию - Учебное пособие. / Под ред. Скрыля С.В. — 2-е изд. — Воронеж: Воронежский институт МВД России, 2008. — 64 с. – стр. 4-6

- неправомерный доступ к ресурсам и услугам систем связи общего пользования;
- контрактный доступ (преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом контрактных условий оплаты);
- технический доступ (неправомерное изменение (клонирование) телефонных трубок или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок).

Актуальной для теории и практики является разработка концептуальной модели, развертывания системы противодействия киберпреступности, ориентированной на эффективное решение задач мониторинга, прогноза, предупреждения, профилактики, выявления, пресечения, раскрытия и расследования киберпреступлений, в том числе разработка требований к методам и средствам судебной компьютерно-технической экспертизы и соответствующих пакетов прикладных программ судебно-экспертного исследования компьютерных систем[23].

[23] Леонов А.П. Актуальные проблемы информационной безопасности в контексте глобализации - Минск: Академия МВД, 2015. — 5 с. — с. 4.

Информационное законодательство РФ

Информационное законодательство РФ.

Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации включают:

- Законы Российской Федерации;
- Указы Президента Российской Федерации и утверждаемые этими указами нормативные документы;
- Постановления Правительства Российской Федерации и утверждаемые этими постановлениями нормативные документы (Положения, Перечни и т.п.);
- Государственные и отраслевые стандарты;
- Положения, Порядки. Руководящие документы и другие нормативные и методические документы уполномоченных государственных органов (Гостехкомиссии России, ФАПСИ, ФСБ).

Федеральные законы и другие нормативные акты предусматривают:

– разделение информации на категории свободного и ограниченного доступа, причем информация ограниченного доступа подразделяется на:

- отнесенную к государственной тайне
- отнесенную к служебной тайне (информацию для служебного пользования), персональные данные (и другие виды тайн);
- другую информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;

– *правовой режим защиты информации,* неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу, устанавливаемый:

– в отношении сведений, отнесенных к государственной тайне, – уполномоченными государственными органами на основании Закона Российской Федерации «О государственной тайне» (от 21.07.93 г. N 5485-1);

– в отношении конфиденциальной документированной информации – собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации «Об информации, информатизации и защите информации» (от 20.02.95 г. N 24-ФЗ);

– в отношении персональных данных – отдельным федеральным законом;

– *лицензирование деятельности* предприятий, учреждений и организаций в области защиты информации;

– *аттестование* автоматизированных информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);

– *сертификацию средств защиты* информации и средств контроля эффективности защиты, используемых в АС;

– возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;

– создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;

– определение прав и обязанностей субъектов в области защиты информации[24].

Фрагменты федерального закона от 27.07.2006 N 149-ФЗ (ред. от 09.03.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 20.03.2021)

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ
И О ЗАЩИТЕ ИНФОРМАЦИИ
Принят
Государственной Думой
8 июля 2006 года
Одобрен
Советом Федерации
14 июля 2006 года

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

[24] Соловьев А.А., Метелев С.Е., Зырянова С.А. Защита информации и информационная безопасность - Учебник. — Омск: Изд-во Омского института (филиала) РГТЭУ, 2011. – 426 с. – с. 23

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.
2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.
Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено
1. В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (далее - реестр).
2. В реестр включаются:
1) доменные имена и (или) указатели страниц сайтов в сети "Интернет", содержащих информацию, распространение которой в Российской Федерации запрещено;
2) сетевые адреса, позволяющие идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.
3. Создание, формирование и ведение реестра осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.
4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра оператора реестра - организацию, зарегистрированную на территории Российской Федерации.

5. Основаниями для включения в реестр сведений, указанных в части 2 настоящей статьи, являются:
1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети "Интернет":
а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;
б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;
в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;
г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;
д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" и Федерального закона от 11 ноября 2003 года N 138-ФЗ "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети "Интернет" и иных средств связи;
е) информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;
ж) информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

з) информации, содержащей предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, розничная торговля которыми ограничена или запрещена в соответствии с законодательством об обращении лекарственных средств, и (или) информации, содержащей предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, лицами, не имеющими лицензии и разрешения на осуществление такой деятельности, если получение лицензии и разрешения предусмотрено законодательством об обращении лекарственных средств;
2) решение суда о признании информации, распространяемой посредством сети "Интернет", информацией, распространение которой в Российской Федерации запрещено;
3) постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети "Интернет", порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.
6. Решение о включении в реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено, может быть обжаловано владельцем сайта в сети "Интернет", провайдером хостинга, оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", в суд в течение трех месяцев со дня принятия такого решения.
7. Незамедлительно с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети "Интернет" в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети "Интернет" и уведомить его о необходимости удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.
8. Незамедлительно с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети "Интернет" в реестр владелец сайта в сети "Интернет" обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети "Интернет" провайдер хостинга обязан ограничить доступ к такому сайту в сети "Интернет" незамедлительно.

9. В случае непринятия провайдером хостинга и (или) владельцем сайта в сети "Интернет" мер, указанных в частях 7 и 8 настоящей статьи, сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, включается в реестр.
10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к такому сайту в сети "Интернет", за исключением случая, предусмотренного абзацем третьим пункта 5.1 статьи 46 Федерального закона от 7 июля 2003 года N 126-ФЗ "О связи".
11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра исключает из реестра доменное имя, указатель страницы сайта в сети "Интернет" или сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", на основании обращения владельца сайта в сети "Интернет", провайдера хостинга или оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", не позднее чем в течение трех дней со дня такого обращения после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено, либо на основании вступившего в законную силу решения суда об отмене решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о включении в реестр доменного имени, указателя страницы сайта в сети "Интернет" или сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет".
12. Порядок взаимодействия оператора реестра с провайдером хостинга и порядок получения доступа к содержащейся в реестре информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

13. Порядок ограничения доступа к сайтам в сети "Интернет", предусмотренный настоящей статьей, не применяется к информации, порядок ограничения доступа к которой предусмотрен статьей 15.3 настоящего Федерального закона.
14. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра в течение суток с момента получения решений, указанных в подпунктах "а", "в" и "ж" пункта 1 части 5 настоящей статьи, уведомляет по системе взаимодействия об этом федеральный орган исполнительной власти в сфере внутренних дел.
Статья 15.3. Порядок ограничения доступа к информации, распространяемой с нарушением закона
1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, информационных материалов иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации в соответствии с Федеральным законом от 28 декабря 2012 года N 272-ФЗ "О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации", сведений, позволяющих получить доступ к указанным информации или материалам (далее - распространяемая с нарушением закона информация), включая случай поступления уведомления о распространяемой с нарушением закона информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители обращаются в федеральный орган исполнительной власти, осуществляющий функции по

контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с требованием о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

1.1. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи и поступившего в отношении недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, которая размещена на информационном ресурсе, зарегистрированном в соответствии с Законом Российской Федерации от 27 декабря 1991 года N 2124-1 "О средствах массовой информации" в качестве сетевого издания (далее - сетевое издание), незамедлительно уведомляет редакцию сетевого издания о необходимости удаления указанной информации и фиксирует дату и время направления такого уведомления редакции сетевого издания в соответствующей информационной системе.

1.2. Незамедлительно с момента получения от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, уведомления, указанного в части 1.1 настоящей статьи, редакция сетевого издания обязана удалить информацию, указанную в части 1.1 настоящей статьи.

1.3. В случае, если редакция сетевого издания незамедлительно не удалила информацию, указанную в части 1.1 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к сетевому изданию, в котором размещена информация, указанная в части 1.1 настоящей статьи. Данное требование должно содержать доменное имя

сайта в сети "Интернет", сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать такую информацию.
1.4. После получения по системе взаимодействия требования, указанного в части 1.3 настоящей статьи, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", незамедлительно обязан ограничить доступ к сетевому изданию, в котором размещена информация, указанная в части 1.1 настоящей статьи, за исключением случая, предусмотренного абзацем третьим пункта 5.1 статьи 46 Федерального закона от 7 июля 2003 года N 126-ФЗ "О связи".
1.5. В случае ограничения доступа к сетевому изданию в порядке, предусмотренном частями 1.1 - 1.4 настоящей статьи, возобновление доступа к сетевому изданию производится в соответствии с порядком, предусмотренным частями 5 - 7 настоящей статьи.
2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи, за исключением случаев, предусмотренных частями 1.1 - 1.4 настоящей статьи, незамедлительно:
1) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, в том числе к сайту в сети "Интернет", на котором размещена распространяемая с нарушением закона информация. Данное требование должно содержать доменное имя сайта в сети "Интернет", сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать такую информацию;
2) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети "Интернет", указанного информационного ресурса, обслуживающего владельца сайта в сети "Интернет", на котором размещена распространяемая с нарушением закона информация;
3) направляет провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети "Интернет", на котором размещена распространяемая с нарушением закона информация, а также указателей страниц сайта в сети "Интернет", позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

4) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.
3. После получения по системе взаимодействия требования федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети "Интернет", на котором размещена распространяемая с нарушением закона информация, за исключением случая, предусмотренного абзацем третьим пункта 5.1 статьи 46 Федерального закона от 7 июля 2003 года N 126-ФЗ "О связи".
4. Незамедлительно с момента получения уведомления, указанного в пункте 3 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 2 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить распространяемую с нарушением закона информацию.
4.1. В течение суток с момента получения от провайдера хостинга или иного указанного в пункте 2 части 2 настоящей статьи лица уведомления о необходимости удалить распространяемую с нарушением закона информацию владелец информационного ресурса обязан удалить такую информацию. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 2 части 2 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу незамедлительно по истечении суток с момента получения уведомления, указанного в пункте 3 части 2 настоящей статьи.
5. В случае, если владелец информационного ресурса удалил распространяемую с нарушением закона информацию, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.
6. После получения уведомления, указанного в части 5 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой

информации, массовых коммуникаций, информационных технологий и связи, обязан незамедлительно уведомить по системе взаимодействия оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", о возобновлении доступа к информационному ресурсу, в том числе к сайту в сети "Интернет".

7. После получения уведомления, указанного в части 6 настоящей статьи, оператор связи незамедлительно возобновляет доступ к информационному ресурсу, в том числе к сайту в сети "Интернет", за исключением случая, предусмотренного частью 7.1 настоящей статьи.

7.1. В случае, если доступ к информационному ресурсу, в том числе к сайту в сети "Интернет", был ограничен федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в соответствии с абзацем третьим пункта 5.1 статьи 46 Федерального закона от 7 июля 2003 года N 126-ФЗ "О связи", возобновление доступа к информационному ресурсу, в том числе к сайту в сети "Интернет", осуществляется данным органом после получения уведомления, указанного в части 5 настоящей статьи, и проверки его достоверности.

8. Предусмотренный настоящей статьей порядок не применяется в случае обнаружения недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, на информационном ресурсе, указанном в статье 10.4 настоящего Федерального закона.

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Военная, государственная, коммерческая тайна. Доктрина информационной безопасности

Государственная и коммерческая тайна.

Согласно Закону о коммерческой тайне под ***коммерческой тайной*** понимается некоторая информация либо формула, не являющаяся общеизвестной. В отношении ПО Закон о коммерческой тайне может применяться для защиты программ, разрабатываемых под конкретные требования клиента[25].

Тайна государственная – это защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение (утрата) которых может нанести ущерб безопасности Российской Федерации. Необходимость отнесения сведений к государственной тайне определяется министерствами и ведомствами в соответствии с разграничением полномочий между ними и с помощью специальных экспертных комиссий.

Информационная война

Одним из главных фронтов современных войн является информационный фронт. В литературе при использовании термина «информационная война» до сих пор наблюдается смешение смыслов. Одни авторы под информационной войной понимают комплекс мероприятий по уничтожению, подавлению или нарушению функционирования систем получения, обработки, хранения и передачи информации противника, а также по защите аналогичных своих систем. Другие этим же термином обозначают мероприятия, направленные на формирование у целевых аудиторий такого восприятия окружающего мира, которое способствовало бы успешному достижению собственных целей войны и препятствовало достижению аналогичных целей противником. Учитывая то, что в первом понятии

[25] Артемов А.В. Информационная безопасность. Курс лекций - М.: Академия безопасности и выживания, 2014. — 161 с. – с. 114

объектом воздействия является техника, а во втором - человеческая психика, было бы оправданно в первом говорить об «информационно-техническом противоборстве», а во втором - об «информационно-психологическом противоборстве», которые представляют собой два аспекта информационной войны[26].

Методы информационной войны:

1. Отключение исторической памяти
2. Выдергивание из контекста
3. Подмена понятий
4. Манипуляция числами

Виды информационной войны:

Командно-управленческая война в качестве основного объекта воздействия рассматривает каналы связи между командованием и исполнителями. Перерезая «шею» (каналы связи), нападающий изолирует «голову» от «туловища». Утверждается, что это лучше, нежели просто убивать «голову». Сам по себе таков подход не нов, например: Интернет (вернее его предшественник АрпаНЕТ) создавался как оборонный вариант этой войны («рассредоточенная шея»).

Разведывательная война имеет целью сбор важной в военном отношении информации и защиту собственной.

Электронная война направлена против средств электронных коммуникаций – радиосвязи, радаров, компьютерных сетей. Ее важнейшей составляющей называется криптография, позволяющая осуществлять шифрование и расшифровку электронной информации.

Психологическая война осуществляется путем пропаганды, «промывания мозгов» и другими методами информационного воздействия на население.

М. Либицки выделяет 4 составляющие психологической войны: подавление воли; деморализация вооруженных сил; дезориентация командования; Kulturkampf (война культур). Kulturkampf собственно и предполагает «промывание мозгов», когда идеи, внушаемые агрессором, становятся доминирующими в общественной мысли и морали жертвы через глобальное информационное воздействие спутникового телевидения, новостных выпусков CNN, сети Интернет и т.д.

[26] Соловьев А.А., Метелев С.Е., Зырянова С.А. Защита информации и информационная безопасность - Учебник. — Омск: Изд-во Омского института (филиала) РГТЭУ, 2011. – 426 с. – с. 383

Хакерская война имеет целями тотальный паралич сетей, перебои связи, введение ошибок в пересылку данных, хищение информации, хищение услуг за счет несанкционированных подключений к сетям, их тайный мониторинг, несанкционированный доступ к закрытым данным. Для достижения этих целей используются различные программные средства: вирусы, «троянские кони», «логические бомбы», средства перехвата и анализа «чужого» сетевого трафика.

Экономическая информационная война. М. Либицки выделяет две ее формы – информационную блокаду (перекрытие каналов коммерции) и техно-империализм (метод самих США).

Кибер-война предполагает использование информационных систем против «виртуальных личностей» (отражения реальных личностей и организаций в сети Интернет, а равно данные о личностях и организациях, размещенные в сети) для захвата размещенных в автоматизированных системах сведений, чтобы затем выследить реальную цель, либо шантажировать ее. Особенности информационной войны в ее отличии от войны «горячей» убедительно показаны в работах С.П. Расторгуева. Так, для войны в ее обычном понимании – «горячей войны» четко определены противостоящие стороны, существуют понятия начала и окончания войны, линии фронта. Противостоящие стороны, как правило, описываются одинаковыми моделями, а исход войны во многом определяется соотношением военных потенциалов сторон. Для информационной войны – «холодной войны» возможно определить только жертву нападения (причем уже по последствиям акта агрессии), понятия начала и окончания применимы лишь к отдельным операциям информационной войны. В информационной войне нет линии фронта, действия обороняющейся и наступающей сторон описываются по различным моделям, а успех проводимых информационных операций не имеет прямой связи с соотношением военных потенциалов сторон. [27].

Информационное оружие и информационное воздействие.

Основным средством ведения информационной войны является информационное оружие. Информационное оружие – это совокупность средств и методов, позволяющих похищать, искажать или уничтожать информацию, ограничивать или прекращать доступ к ней законных пользователей, нарушать работу или выводить из строя

[27] Аникин Д.В. Информационная безопасность и защита информации - СПб.: Институт электронного обучения Санкт-Петербургского университета технологий управления и экономики, 2011. — 269 с. – с. 36-37

телекоммуникационные сети и автоматизированные системы, используемые в обеспечении жизнедеятельности общества и государства. Помимо военной сферы информационное оружие активно применяется для подавления управленческой, экономической, банковской, социальной и иных областей. К видам информационного оружия принято относить:

Средства массовой информации, под которыми принято понимать периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации. Под массовой информацией понимаются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Психотронные генераторы – это устройства, осуществляющие воздействие на человека путем передачи информации через внечувственное (неосознаваемое) восприятие. Например, уже давно установлено, что разные органы человека имеют собственные резонансные частоты, используя которые можно воздействовать на психикофизиологическое состояние индивида или коллектива людей, вызывая у них страх, подавленность или другие чувства.

Психотропные препараты – это лекарственные (наркотические) средства, которые способны вызывать состояние зависимости, оказывать стимулирующее или депрессивно воздействие на центральную нервную систему, вызывая галлюцинации или нарушение моторной функции организма, под воздействием которых происходит нарушение мышления, меняется настроение, поведение.

Средства радиоэлектронной борьбы (РЭБ) – это средства для выявления и радиоэлектронного подавления систем управления войсками и оружием противника, его систем разведки и навигации, а также средства для обеспечения устойчивой работы своих систем.

Средства специального программно-технического воздействия (СПТВ) – программные, аппаратные или программно-аппаратные средства, с использованием которых может быть осуществлено несанкционированное копирование, искажение, уничтожение информации, ее передача за пределы контролируемой зоны или блокирование доступа к ней[28].

[28] Аникин Д.В. Информационная безопасность и защита информации - СПб.: Институт электронного обучения Санкт-Петербургского университета технологий управления и экономики, 2011. — 269 с. – с. 32-34

ГЛОССАРИЙ

Аутентификация – проверка подлинности документов, информации, передаваемых по запросу пользователей или иных лиц.

Безопасность – защищенность жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, состояние, при котором чему-либо или кому-либо не угрожает опасность.

Доступ к информации несанкционированный – случайное или преднамеренное овладение конфиденциальными сведениями и возможное опасное воздействие на них лиц, не имеющих права доступа к конкретной *защищаемой информации.* Доступ, не санкционированный полномочным должностным лицом, считается незаконным. Случайный несанкционированный доступ *к конфиденциальной информации* возникает в силу обстоятельств или в результате безответственности персонала, работающего с документами, *информационными ресурсами ограниченного доступа.* Лицо, случайно получившее знание конфиденциальных сведений, обычно не заинтересовано в их запоминании и использовании. Преднамеренный несанкционированный доступ к конфиденциальной информации осуществляет злоумышленник, который целенаправленно организует канал *несанкционированного доступа к* интересующей его информации. Злоумышленник, получивший информацию, имеет возможность совершить с. ней противоправные действия, использовать в своих целях, нарушить целостность информации или ее сохранность, уничтожить носитель. *Владелец информационных ресурсов обязан оповещать собственника этих ресурсов о* всех фактах нарушения *режима конфиденциальности* информации.

Идентификация пользователя – отождествление лиц по их характеристикам или путем опознавания по приметам или документам в целях определение полномочий, связанных с доступом к конфиденциальной информации. Присвоение имени пользователю информационной системы, потребителю информации.

Интеллектуальная собственность – исключительное право юридического или физического лица на результаты интеллектуальной деятельности, творческого труда *(информационный продукт),* имеющего конкретную ценность для *собственника или владельца этих* результатов. Обычно выделяются два вида информации, интеллектуально ценной для предпринимателя, его собственной, частной информации: а) техническая или

технологическая (ценная идея, технологическое новшество, ноу-хау, новое знание, параметры, формулы, рецептуры, результаты испытаний опытных образцов и т. п.) и б) деловая (творческое решение управленческой или иной проблемы, результаты исследования рынка, экономические показатели, прогнозы, стратегия действий на рынке, реорганизация структуры фирмы и т. п.).

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Документирование информации (создание официального документа) является обязательным условием включения информации в информационные ресурсы. По принадлежности к тому или иному виду собственности информационные ресурсы могут быть государственными или негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной и исполнительной власти, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных объединений, предпринимательских структур. Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации. В соответствии с интересами обеспечения национальной и экономической безопасности и степенью ценности для государства, а также правовыми, экономическими и другими интересами предпринимательских (негосударственных) структур информационные ресурсы могут быть: а) открытыми, т. е. общедоступными, используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми на конференциях, в выступлениях, интервью и т. п., и б) *ограниченного доступа* и использования.

Криптография – тайнопись, система разнообразных способов изменения формы отображения информации (текста, речи), позволяющих сделать содержание информации непонятным для лиц, не владеющих знанием использованного шифра. Криптографические методы представляют собой *шифрование,* кодирование, сжатие, расчленение (разнесение) информации. Криптография входит составной частью в понятие криптологии, в которое включается также криптоанализ – дешифрование текста или речи известным ключом или без него.

Персональные данные – информация о гражданах, лицах, особах, персонах, личностях, персоналиях, т. е. любая, в том числе недокументированная, информация, относящаяся к конкретному человеку.

Субъектами персональных данных являются граждане РФ, иностранные граждане и лица без гражданства, находящиеся на территории России, к личности которых относятся соответствующие персональные данные. Персональные (личные) данные всегда входят в категорию конфиденциальной информации. Не допускается сбор, передача, уничтожение, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей *личную, семейную тайну,* тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Запрещается ограничение прав граждан как результат использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности. Персональные данные находят отражение прежде всего в *персональных* и других документах кадровой службы, в информационно-документационной системе, обеспечивающей управление персоналом.

Противодействие злоумышленнику – целенаправленное создание неблагоприятных условий и трудно преодолимых препятствий (рубежей) для лица, пытающегося совершить несанкционированный доступ и овладение конфиденциальной информацией фирмы. Может быть пассивным и активным. При пассивном противодействии *система защиты информации* функционирует в обычном режиме, ведется плановая аналитическая и контрольная работа с *источниками и каналами распространения информации, организационными и техническими каналами возможного несанкционированного доступа* к конфиденциальной информации. Активное противодействие предполагает подключение дополнительных организационных и *технических методов защиты* информации (например, закрытие доступа к определенным категориям информации, организацию усиленной охраны здания и помещений, ограничение деловых связей фирмы и др.).

Средства несанкционированного доступа к информации – специально изготовленные технические средства промышленного шпионажа: приборы, оборудование, системы приборов и средств связи, предназначенные для создания контакта с *источником конфиденциальной информации* или *каналом объективного распространения информации* и образования *технического канала утечки этой информации* (видео– и аудиооборудование, бинокли, лазерные приборы, радиозакладки и др.).

Тайна государственная – защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной,

контрразведывательной и оперативно-розыскной деятельности, распространение (утрата) которых может нанести ущерб безопасности Российской Федерации. Необходимость отнесения сведений к государственной тайне определяется министерствами и ведомствами в соответствии с разграничением полномочий между ними и с помощью специальных экспертных комиссий.

Уязвимость информации – объективное свойство информации подвергаться различного рода воздействиям (опасностям, угрозам), нарушающим ее целостность, достоверность и *конфиденциальность.* Воздействия носят дестабилизирующий по отношению к информации характер и приводят *к утрате носителя конфиденциальной информации или утрате конфиденциальности информации.* Уровень уязвимости информации находится в прямой зависимости от степени совершенства применяемой в фирме *системы защиты информации,* перекрытия этой системой всей сферы возможных *угроз* и предполагаемых *сигналов несанкционированного доступа к информации.*

Шифрование – криптографическое (математическое, алгоритмическое) преобразование информации с целью получения шифрованного текста или устной речи (см. также *Криптография).*

Шпионаж – похищение, добывание, собирание и передача с целью корыстного использования или выдачи конкуренту (противнику) сведений, составляющих *тайну.*

СПИСОК ЛИТЕРАТУРЫ

Нормативные акты

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс».

2. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Консультант Плюс».

3. Закон РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2023) "О государственной тайне"// СПС «Консультант Плюс».

4. Конституция Российской Федерации принята всенародным голосованием 12 декабря 1993 г. (в действующей редакции) // СПС «Консультант Плюс».

5. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в действующей редакции) // СПС «Консультант Плюс».

6. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (в действующей редакции) // СПС «Консультант Плюс».

Учебники и научные статьи

7. Альтовский Е. Настольная книга кибердиссидента - М.: МОО «Информация для всех», 2013. — 16 с.

8. Амелин Р.В. Информационная безопасность - Саратов: УЦ «Новые технологии в образовании». - 121 с.

9. Артемов А.В. Информационная безопасность. Курс лекций. - М.: Академия безопасности и выживания, 2014. — 161 с.

10. Ахметова С.Г. Информационная безопасность. - Учеб.-метод. пособие. – Пермь : Изд-во Перм. нац. исслед. политехн. ун-та, 2013. – 123 с.

11. Бирюков А.А. Информационная безопасность: защита и нападение. - ДМК Пресс, 2012. — 476 с.

12. Василенко В.А., Женса А.В. Информационная безопасность и защита информации - М.: РХТУ им. Д.И. Менделеева, 2016. — 171 с.

13. Васильева И.Н. Управление информационной безопасностью. - СПб.: Изд-во СПбГЭУ, 2014. — 82 с.

14. Войтик А.И., Прожерин В.Г. Экономика информационной безопасности. - Учебное пособие. – СПб.: НИУ ИТМО, 2012. – 120 с.

15. Ганжа В.А., Сидорик В.В., Чичко О.И. Компьютерные сети. Информационная безопасность и сохранение информации. - Учебно—методическое пособие. — Минск: БГУИР, 2014. — 128 с.

16. Горюхина Е.Ю., Литвинова Л.И., Ткачева Н.В. Информационная безопасность - Воронеж: Воронежский ГАУ, 2015. — 220 с.

17. Громов Ю.Ю., Иванова О.Г., Мартемьянов Ю.Ф., Букурако Ю.К., Однолько В.Г. Методы организации защиты информации. - Учебное пособие. – Тамбов: Изд.-во ТГТУ, 2013. – 80 с.

18. Демидов Д.Г., Швечкова О.Г., Москвитина О.А. и др. Защита информации с использованием механизмов электронной цифровой подписи. - Учебно-метод. пособие. — М.: МГУП имени Ивана Федорова, 2014. — 53 с.

19. Джонс Кейт Дж., Шема Майк, Джонсон Бредли С. Инструментальные средства обеспечения безопасности. - 2-е изд. — М.: НОУ "Интуит", 2016. — 914 с.

20. Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государства - СПб.: ГИКиТ, 2016. — 396 с.

21. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста - М.: ДМК-Пресс, 2013. – 656 с.

22. Климов С.М., Сычев М.П., Астрахов А.В. Противодействие компьютерным атакам. Методические основы - Электронное учебное издание. — М.: МГТУ имени Н.Э. Баумана, 2013. — 108 с.

23. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью - Учебное пособие для вузов. — 2-е изд., испр. — М.: Горячая линия-Телеком, 2014. — 244 с.

24. Лапонина О.Р. Криптографические основы безопасности. - 2-е изд. — М.: Национальный Открытый Университет ИНТУИТ, 2016. — 242 с.

25. Леонов А.П. Актуальные проблемы информационной безопасности в контексте глобализации - Минск: Академия МВД, 2015. — 5 с.

26. Лукацкий А. Тренды информационной безопасности в России в 2015-м году - М.: Cisco, 2014. — 40 с.

27. Лыньков Л.М., Голиков В.Ф., Борботько Т.В. Основы защиты информации и управления интеллектуальной собственностью. - Учебно-методическое пособие. — Минск: БГУИР, 2013. — 243 с.

28. Манжуева О.М. Парадигма информационной безопасности - Монография. — Улан-Удэ: Издательство Бурятского госуниверситета, 2013. — 152 с.

29. Мельников В.П. Информационная безопасность и защита информации - Учебное пособие для студентов учреждения высшего

профессионального образования. — 6-е изд.,стереп. — М.: Академия, 2012 — 330 с.

30. Нестеров С.А. Основы информационной безопасности. - Учебное пособие — 3-е изд., стер. — СПб.: Лань, 2017. — 324 с.

31. Парошин А.А. Информационная безопасность: стандартизированные термины и понятия - Владивосток: Дальневосточный университет, 2010. — 216 с.

32. Платонов А.А. Информационная безопасность - Учебное пособие. — Волгоград: ВолгГАСУ, 2016. — 69 с.

33. Прозоров Андрей. Нормативная база ИБ. - Москва: RISA, 2014. — 55 с.

34. Проскурин В. Защита в операционных системах. - М.: Горячая линия - Телеком, 2014. — 192 с.

35. Пулко Т.А. Введение в информационную безопасность. - Учебно-методическое пособие. — Минск : БГУИР, 2016. — 156 с.

36. Пулко Т.А. Введение в информационную безопасность. - Учебно-методическое пособие. – Минск : БГУИР, 2016. – 156 с.

37. Слесарев С. Вся правда о паролях. - Интернет-издание, 2013. — 20 с.

38. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. - М.: РЭУ им. Г.В. Плеханова, 2017. — 207 с.

39. Теплов Э.П. и др. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательств и защиты от манипуляций. - Теплов Э.П., Гатчин Ю.А., Ныркова А.П., Сухостат В.В. — Учебное пособие. – СПб: Университет ИТМО, 2016. – 120 с.

40. Царев Е. и др. Первое комплексное исследование рынка информационной безопасности России-2013 год

41. Шаньгин В.Ф. Информационная безопасность. - М.: ДМК Пресс, 2014. — 712 с.