Juristic 300

ПДн_БД

Задание

Пару минут назад мы получили шифротелеграмму, в ней написано, что мы “не боги, и законы по защите Пдн распространяются и на” нас! Не могли бы Вы выбрать необходимые мероприятия (необходимо перечислить в порядке возрастания номеров через запятую)?

Какие исходные данные? Наша база Пдн относится только к нашим работникам и находится вся в этом здании, выход в интернет есть, через 1 шлюз.

Какие действия доступны с данными? чтение, поиск, запись, удаление, сортировка, копирование, модификация, передача.

К БД имеют доступ только лица, указанные в Приказе № 678.56/12, сторонним пользователям без предварительной обработки мы информацию не предоставляем!

Вот пример нашей базы данных:

Иванов Михаил Яковлевич	1873	--	Москва	Иванова Маргарита Петровна
Дмитриев Александр Александрович	1880	--	Владимир	холост
Петров Пётр Иванович	1888	--	Красноярск	холост
Мелехов Иван Михайлович	1891	инв. II	Киев	холост

Наши специалисты подготовили еще 2 файла для Вас:

- Вероятность реализации угроз безопасности ПДн
- Оценка опасности угроз для Пдн

Ах да, данные обезличиваются только при предоставлении в другие организации!

Мероприятия:

1. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

2. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

3. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

5. Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

6. Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных

7. Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему

8. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

9. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

10. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации

11. Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки

12. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

13. Обеспечение доверенной загрузки средств вычислительной техники

14. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

15. Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

16. Управление доступом к машинным носителям персональных данных

17. Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных

18. Контроль ввода (вывода) информации на машинные носители персональных данных

19. Контроль подключения машинных носителей персональных данных

20. Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания

21. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

22. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти

23. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

24. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

25. Обнаружение вторжений

26. Обновление базы решающих правил

27. Контроль состава технических средств, программного обеспечения и средств защиты информации

28. Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных

29. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы

30. Управление изменениями конфигурации информационной системы и системы защиты персональных данных

Решение

На основе «МЕТОДИКИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ» определяем исходный уровень защищенности ИСПДн:

1. По территориальному размещению: Локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования: ИСПДн с одноточечным выходом в общественные сети	–	+	–
3. По встроенным (легальным) операциям с записями баз персональных данных: чтение, поиск, запись, удаление, сортировка копирование, модификация, передача	–	–	+
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники Общества	+	–	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	–	+	–
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: не предостав. инф-ю сторонним пользователям	+	–	–

Делаем вывод: ИСПДн имеет **средний** уровень исходной защищенности, так как более 70% характеристик соответствуют уровню не ниже «средний». Показатель исходной защищенности $\mathbf{Y_1=5}$.

Определяем вероятность реализации угроз безопасности Пдн и коэффициент Y_2:

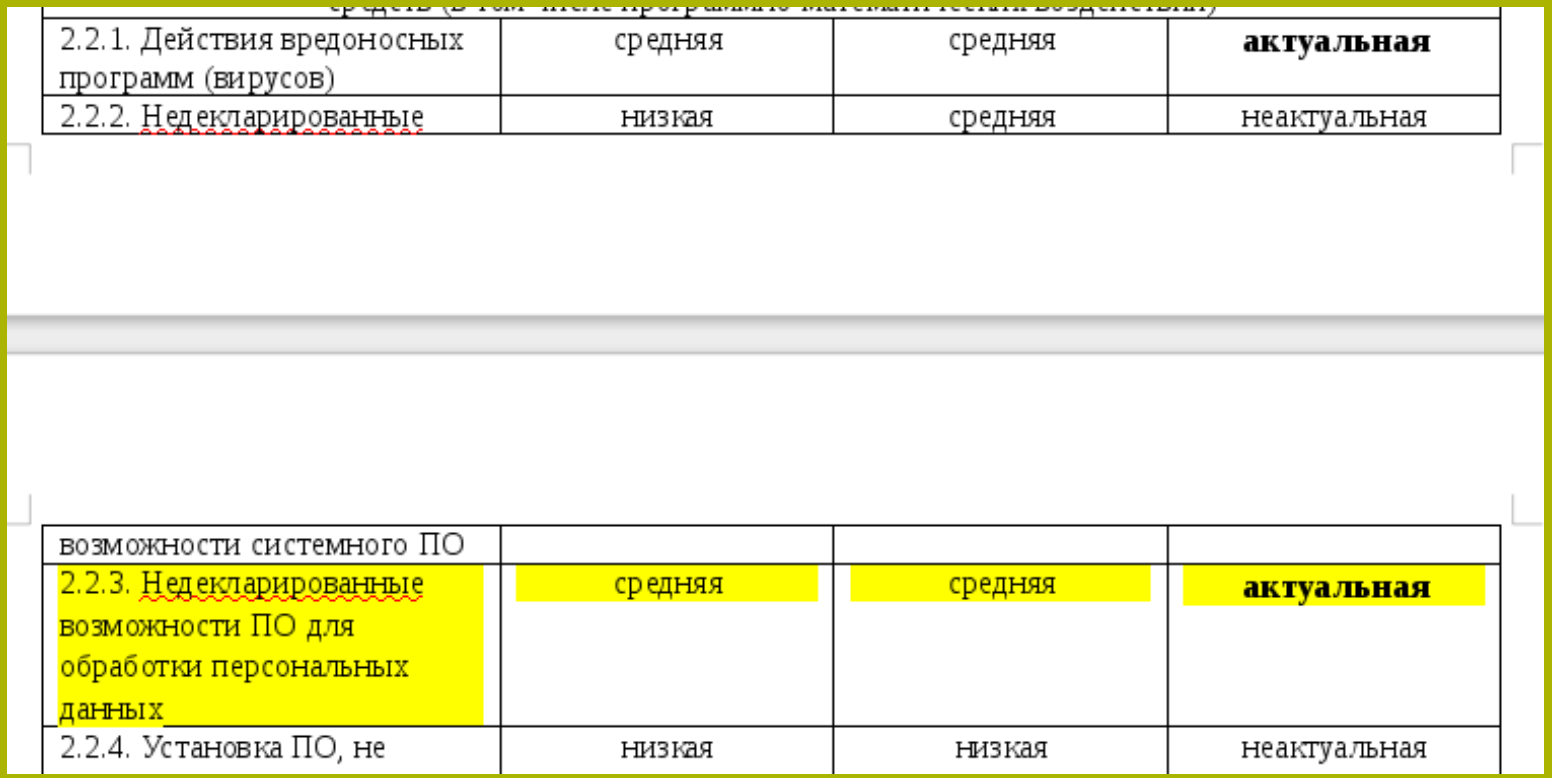
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0	маловероятная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Adjust table column	маловероятная
2.1.7. Несанкционированное отключение средств защиты	0	маловероятная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
2.2.1. Действия вредоносных программ (вирусов)	2	низкая
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	2	низкая
2.2.3. Недекларированные возможности ПО для обработки персональных данных	5	средняя
2.2.4. Установка ПО, не связанного с исполнением служебных обязанностей	0	маловероятная

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается **коэффициент реализуемости угрозы** (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$.

связи		
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
2.2.1. Действия вредоносных программ (вирусов)	0,35	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,35	средняя
2.2.3. Недекларированные возможности ПО для обработки персональных данных	0,50	средняя
2.2.4. Установка ПО, не связанного с исполнением служебных обязанностей	0,25	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности		

На основе данных об опасности угрозы и коэффициента реализуемости делаем вывод о её актуальности.

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная



2.2.1. Действия вредоносных программ (вирусов)	средняя	средняя	**актуальная**
2.2.2. Недекларированные возможности системного ПО	низкая	средняя	неактуальная
2.2.3. Недекларированные возможности ПО для обработки персональных данных	средняя	средняя	**актуальная**
2.2.4. Установка ПО, не	низкая	низкая	неактуальная

Видим, что нас интересуют только угрозы 2-го типа (связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе).

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Тогда на основе Постановления Правительства РФ № 1119 мы можем смело определить требуемый уровень защищенности – 2 УЗ, зная, что обрабатываем специальную категорию Пдн (инвалидность).

Теперь на основе Приказа ФСТЭК № 21 определяем необходимые организационные и технические меры по обеспечению безопасности персональных данных для 2УЗ:

+ 1. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

+ 2. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

+ 3. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

+ 4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

+ 5. Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

– 6. Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных

– 7. Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему

– 8. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

+ 9. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

+ 10. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации

– 11. Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки

+ 12. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

+ 13. Обеспечение доверенной загрузки средств вычислительной техники

+ 14. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

– 15. Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

+ 16. Управление доступом к машинным носителям персональных данных

– 17. Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных

– 18. Контроль ввода (вывода) информации на машинные носители персональных данных

– 19. Контроль подключения машинных носителей персональных данных

+ 20. Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания

+ 21. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

– 22. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти

+ 23. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

– 24. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

+ 25.Обнаружение вторжений

+ 26. Обновление базы решающих правил

+ 27. Контроль состава технических средств, программного обеспечения и средств защиты информации

+ 28. Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных

– 29. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы

+ 30. Управление изменениями конфигурации информационной системы и системы защиты персональных данных

Флаг

Таким образом, получаем флаг:

«1,2,3,4,5,9,10,12,13,14,16,20,21,23,25,26,27,28,20»