КТ 3

Работу выполнили студенты 1-го курса физического факультета:

Даниил Блохин ФИЗ-2

Леготкин Михаил ФИЗ-1

Описание информационной системы (состав оборудования и ПО)

- Сеть банка АКБ «Банк»;
- 10 ПЭВМ и один сервер;
- Есть подключение в ЛВС(локальной вычислительной сети), имеющей выход в сеть Интернет;
- Расположена в отдельном здании внутри охраняемой территории (с учетом возможности посещения клиентами операционных помещений банка).

Перечень возможных угроз

При обработке ПДн в локальных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих **УБПДн**:

- угрозы **утечки информации по техническим каналам**;
- угрозы **НСД к ПДн, обрабатываемым на автоматизированном рабочем месте**.

Утечки информации по техническим каналам

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

Возникновение **угроз утечки акустической (речевой) информации**, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация **угрозы утечки видовой информации** возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы **утечки информации по каналу ПЭМИН** возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

Угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД, **связанные с действиями нарушителей, имеющих доступ к ИСПДн**, включают в себя угрозы, аналогичные тем, которые реализуются в отдельном АРМ, не имеющем подключения к сетям связи общего пользования:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ.

Угрозы **из внешних сетей** включают в себя:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

Определяем показатель исходной защищенности информационной системы.

Технические и эксплуатационные характеристики ИСПДн		**Уровень защищенности**
1. По территориальному размещению:	локальная ИСПДн, развернутая в пределах одного здания	**Высокий**
2. По наличию соединения с сетями общего пользования:	ИСПДн, имеющая многоточечный выход в сеть общего пользования	**Низкий**
3. По встроенным (легальным) операциям с записями баз персональных данных:	модификация, передача	**Низкий**
4. По разграничению доступа к персональным данным:	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	**Средний**

Технические и эксплуатационные характеристики ИСПДн		Уровень защищенности
5. По наличию соединений с другими базами ПДн иных ИСПДн:	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	**Высокий**
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	**Средний**
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:	ИСПДн, не предоставляющая никакой информации.	**Высокий**

Поскольку ИСПДн имеет низкие уровни защищенности по некоторым пунктам, то высокий уровень ей полностью поставить нельзя, поэтому проверяем, удовлетворяет ли ИСПДн среднему уровню защищенности. Из семи пунктов уровни «средний и выше» имеют пять, средний уровень будет присвоен ИСПДн, усли будет выполняться неравенство:

(N«ср и выше»/N«общ»)*100%>=70%

Из этого выводим (5/7)*100%=71% , из чего следует, что ИСПДн имеет **средний уровень защищенности**, **Y1=5**.

Определяем вероятность реализации угроз

Исходя из данных информационной защищенности ИСПДн и Базовой модели угроз ФСТЭК, определим вероятность реализации угроз безопасности ПДн.

Вероятность угроз утечки акустической информации будет **высокой** (**Y2(А)=10**), поскольку, на мой взгляд, прослушать ПДн клиентов банка представляется очень простым(даже если не удастся услышать кодовые слова карт, можно услышать Фамилию, Имя, Отчество, Адрес, Тлефон и пр. в своих целях, начиная от ограбления, заканчивая похищением человека(если у клиента есть малолетние дети и он с ними пришел в банк).).

Вероятность угрозы утечки видовой информации будет **низкой** (**Y2(В)=2**) , поскольку в помещении находится много сотрудников, есть администратор, который следит за рабочими местами во время отлучки сотрудников, а также многие рабочие места являются закрытыми со стороны клиента стеклами, а экраны развернуты в сторону от клиента-злоумышленника.

Вероятность угрозы утечки информации по каналу ПЭМИН будет **малой** (**Y2(П)=0**), поскольку должны быть приняты, на мой взгляд меры по предотвращению или глушению электромагнитных излучений и наводок.

Вероятность угроз НСД, связанных с действиями нарушителей, имеющих доступ к ИСПДн будет **низкой** (**Y2(НСДИД)=2**), поскольку приняты необходимые меры(описанные для угроз утечки видовой информации), а также личности работников фиксируются(пользователей) и они несут ответственность за действия над ПДн.

Вероятность уроз НСД из внешних сетей будет **высокой** (**Y2(НСДНИД)=10**), поскольку локальная сеть имеет доступ к сети Интернет, а уровень знания ПК, а также угроз, связанных с его использованием у работников(пользователей) низкий.

Определим возможность реализации угроз

Коэффициент реализуемости угрозы Y будет определяется соотношением:

Y=(Y1+Y2)/20

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если 0 <=Y <=0,3, то возможность реализации угрозы признается **низкой**;

если 0,3 < *Y* <= 0,6 , то возможность реализации угрозы признается **средней**;

если 0,6 < *Y* <= 0,8, то возможность реализации угрозы признается **высокой**;

если *Y* > 0,8, то возможность реализации угрозы признается **очень высокой**.

Y(А)=(5+10)/20=0,75 , из чего следует, что возможность реализации угрозы утечки акустической информации является **высокой;**

Y(В)=(5+2)/20=0,35 , из чего следует, что возможность реализации угрозы утечки видовой информации является **средней;**

Y(П)=(5+0)/20=0,25 , из чего следует, что возможность реализации угрозы утечки информации по каналу ПЭМИН является **низкой;**

Y(НСДИД)=(5+2)/20=0,35 , из чего следует, что возможность реализации угроз НСД, связанных с действиями нарушителей, имеющих доступ к ИСПДн является **средней;**

Y(НСДНИД)=(5+10)/20=0,75 , из чего следует, что возможность реализации угроз НСД, связанных с действиями нарушителей, не имеющих доступа к ИСПДн является **высокой;**

Опасность угроз

Оценку опасности угроз, на мой взгляд, лучше рассматривать с позиции массовости воздействия, т.е. количества учетных записей клиентов банка, угроза конфиденциальности, целостности и доступности которым осуществляется при действиях злоумышленника.

Исходя из этого примем, что в случаях угрозы утечки видовой или акустической информации может пострадать один или несколько владельцев ПДн, т.е. **опасность** этих **угроз низкая**.

В остальных же случаях **опасность угроз** будет **высокой**, поскольку могут пострадать данные учетных записей многих(если не всех) владельцев ПДн, а источник угрозы определен несвоевременно.

Актуальность угроз

Выбираем из общего (предварительного) перечня угроз безопасности те, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице.

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

Исходя из таблицы понимаем, что актуальными являются угрозы утечки акустической информации, угрозы утечки информации по каналу ПЭМИН, а также оба вида угроз НСД.

Уровень защищенности ПДн

Исходя из вышеперечисленного занесем данные в таблицу.

Тип актуальной угрозы определяется по наличию или отсутствию в прикладном или системном ПО НДВ(1,2,3 типы).

- Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием НДВ в системном программном обеспечении, используемом в информационной системе.
- Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием НДВ в прикладном программном обеспечении, используемом в информационной системе.
- Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием НДВ в системном и прикладном программном обеспечении, используемом в информационной системе.

Предположим, что мы имеем дело с угрозами 2-го типа.

По данным ПП 1119 устанавливаем, что **уровень защищенности (УЗ) ПДн** для Общедоступных ПДн и Иных категорий ПДн будет **3**-им.

Параметр	**Соответствующие переменные**
Категории персональных данных	Общедоступные ПДн, Иные категории ПДн. (ФИО, адрес, ИНН, паспорт, банковская и финансовая информация)
Категории субъектов	Клиенты банка (не сотрудники оператора)
Количество субъектов	<=5000 (а следовательно <100000)
Тип актуальных угроз	2
Уровень защищенности персональных данных(УЗ ПДн)	Общедоступные – 3-ий, Иные категории – 3-ий.

Состав и содержание мер по обеспечению ИБ (согласно Приказу ФСТЭК №21)

Дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

- проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
- тестирование информационной системы на проникновения;
- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Для обеспечения 3 уровня защищенности персональных данных применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа;
- межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа.

Для обеспечения 1 и 2 УЗ ПДн, а также для обеспечения 3 УЗ ПДн в ИС, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, ПО которых прошло проверку не ниже чем по 4 уровню контроля отсутствия НДВ.

Идентификация и аутентификация пользователей, являющихся работниками оператора;

Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

Защита обратной связи при вводе аутентификационной информации;

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

Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
- Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
- Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
- Регламентация и контроль использования в информационной системе технологий беспроводного доступа
- Регламентация и контроль использования в информационной системе мобильных технических средств
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
- 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
- Определение событий безопасности, подлежащих регистрации, и сроков их хранения
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
- Защита информации о событиях безопасности
- Реализация антивирусной защиты
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
- Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
- Контроль состава технических средств, программного обеспечения и средств защиты информации
- Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
- Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
- Регистрация событий безопасности в виртуальной инфраструктуре
- Реализация и управление антивирусной защитой в виртуальной инфраструктуре
- Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
- Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
- Защита беспроводных соединений, применяемых в информационной системе
- Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
- Управление изменениями конфигурации информационной системы и системы защиты персональных данных
- Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
- Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

Определяем средства защиты информации

- Организационные
- Криптографические
- Технические

Организационные средства защиты информации

Организационные меры представляют собой, в первую очередь, обучение персонала(работников банка) грамотной работе с ПК в различных ситуациях, а также отделению приемных работников от общего холла.

Криптографические средства защиты информации

- «Генератор шума «Старкад-32»
- «Автоматизированное рабочее место для реализации доступа пользователей абонентского пункта к информационным ресурсам сети Интернет «ЗПК – Интернет»
- «Kaspersky Endpoint Security 10 для Windows (Service Pack 1 Maintenance Release 2)»
- «Принтер лазерный «Принтер-Л»
- «Программно-аппаратный комплекс «Маршрутизатор DioNIS TS/FW 16000RM» (исполнения 1, 2)»

Технические средства защиты информации

- система защиты «Гром-ЗИ-4»
- устройство защиты телефонных линий «Сигнал-3»
- устройство активной защиты информации «Волна-4М»
- система акустической и вибрационной защиты «Кабинет»
- фильтр сетевой помехоподавляющий ФСП-1Ф-7А
- устройство защиты громкоговорителей «УЗГ»
- встроенные средства защиты ОС MS Windows

Оценка стоимости

Средство защиты	Цена
«Генератор шума «Старкад-32»	
«Автоматизированное рабочее место для реализации доступа пользователей абонентского пункта к информационным ресурсам сети Интернет «ЗПК – Интернет»	
«Kaspersky Endpoint Security 10 для Windows (Service Pack 1 Maintenance Release 2)»	
«Принтер лазерный «Принтер-Л»	
«Программно-аппаратный комплекс «Маршрутизатор DioNIS TS/FW 16000RM» (исполнения 1, 2)»	
система защиты «Гром-ЗИ-4»	
устройство защиты телефонных линий «Сигнал-3»	
устройство активной защиты информации «Волна-4М»	
система акустической и вибрационной защиты «Кабинет»	
фильтр сетевой помехоподавляющий ФСП-1Ф-7А	
устройство защиты громкоговорителей «УЗГ»	
встроенные средства защиты ОС MS Windows NT 4.0 Workstation (Russian) с пакетом обновления Service Pack 5 (Russian)	
Общая стоимость	

Спасибо за невнимание!