ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4
АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Цель занятия: изучить классификацию угроз безопасности информации, методику их оценки и получить практические навыки по ее применению для заданного информационного объекта.

1 Краткие теоретические сведения

При доступе нарушителя к носителю информации происходит реализация угроз безопасности информации. Под **угрозой безопасности информации** будем понимать воздействия на носитель информации, которые приводят к ущербу. Для того чтобы понять на сколько та или иная угроза является существенной для этого оценивают ущерб, который причиняется вследствие ее реализации.

Ущерб может быть оценен в денежном эквиваленте (например, когда реализация угрозы разглашения данных платежной карточки приводит к потере денежных средств) или категориально (например, ущерб приемлем или ущерб не приемлем). Если человек принимает ущерб, то это означает, что текущая ситуация складывающаяся в информационных отношениях его устраивает.

Информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

Когда ущерб в денежном или категориальном исчислении не приемлем, то требуется обеспечить защиту информации, а точнее ее носителя для минимизации ущерба. Таким образом, необходимость обеспечения безопасности информации обуславливается необходимостью снижения ущерба от ее утраты.

Угрозы по их виду делят на следующие категории:

1. Угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам информационных отношений (создатель, обладатель информации);

2. Угроза целостности – направлена на изменение содержания информации (искажение) или ее уничтожение;

3. Угроза доступности – приводит к нарушению доступа к информации, а также влияет на работоспособность ее носителя;

4. Угроза подлинности – приводит к невозможности однозначно идентифицировать (определить) автора или источник, откуда она получена;

5. Угроза сохранности – ее следствием является не возможность обеспечить такой режим хранения информации, который позволял бы гарантировать ее конфиденциальность, целостность и доступность.

Источниками угроз безопасности информации являются:

1. Человек – вследствие его целенаправленного (преднамеренного) или случайного воздействия на носитель информации;

2. Технические средства обработки информации – их некорректная работа или выход из строя приводит к различным видам угроз;

3. Программное обеспечение – ошибки в нем приводят к не корректной его работе и реализации различных видов угроз безопасности информации;

4. Внешняя среда – стихийные бедствия и другие воздействия на носитель информации, в том числе техногенного характера (отключение электропитания и т.д.), являются причиной реализации угроз безопасности информации.

По мере проявления угрозы безопасности информации делятся на преднамеренные и случайные угрозы.

Преднамеренные угрозы связаны с целенаправленными действиями человека и носят злонамеренный характер.

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программного обеспечения, воздействием внешней среды, а также не злонамеренными действиями человека в силу его некомпетентности или усталости.

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Различают следующие методы защиты информации:

Правовые – определяют порядок регулирования информационных отношений и требования к средствам и системам защиты информации (нормативные правовые акты Республики Беларусь, приказы по организации и политики безопасности).

Организационные – регламентируют методы и способы достижения требований безопасности (изложенные в нормативных правовых актах) и позволяют повысить эффективность применения средств защиты информации.

Технические – обеспечивают конфиденциальность, целостность и доступность информации за счет использования криптографических и технических средств защиты информации.

Для того чтобы обеспечить безопасность информации необходимо использовать правовые, организационные и технические методы. Их одновременное применение свидетельствует о том, что безопасность информации обеспечивается ***комплексно***.

Средства криптографической защиты информации – технические, программные, программно-аппаратные средства, которые реализуют криптографические алгоритмы и протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.

Средства технической защиты информации – имеют техническую, программную или программно-аппаратную реализацию.

Необходимо отметить, что для того чтобы дать однозначный ответ какие из угроз являются наиболее опасными, необходимо оценить ущерб от их реализации. Это позволит обосновать применения определенных методов и средств защиты информации.

Оценка угроз безопасности информации проводится в целях их идентификации для заданного объекта (носителя информации) и определения степени их влияния на этот объект, что позволяет технически и экономически обосновать систему его защиты.

Оценка угроз безопасности информации должна носить систематический характер. Она проводится с использованием экспертного метода. Такой метод заключается в принятии решения экспертом (специалист в определенной области (в данном случай в области информационной безопасности)) на основании его опыта и знаний. Для снижения влияния субъективных факторов на результат оценки, она проводится группой экспертов.

При выполнении оценки угроз безопасности информации необходимо иметь полную информацию об объекте (его назначение, область применения, каким образом он задействован в информационных отношениях). На основании такой информации выполняется непосредственно оценка угроз для заданного объекта.

На ***первом этапе*** определяют, какие конкретно из угроз безопасности информации для данного объекта могут быть реализованы при доступе к нему нарушителя и к какому виду угроз они относятся.

Рассмотрим пример. Предположим, что текстовая информация, написанная от руки, относящаяся к информации распространение и (или) предоставление которой ограничено, содержится на бумажном носителе и этот носитель лежит на столе. Существует еще один аналогичный документ, который хранится в сейфе.

В случае доступа нарушителя к носителю реализуется угроза физического доступа к носителю информации, и она приводит к нарушению конфиденциальности информации содержащейся на этом носителе, если нарушитель ее прочитает. При физическом доступе к носителю информации также возможна угроза доступности информации, так как нарушитель может уничтожить носитель. В рассматриваемом случае угроза целостности информации не является характерной, так как текст написан от руки и внесение любых изменений в существующий документ будет заметно. Для данного случая угроза подлинности также не является характерной. Вместе с тем, так как угрозы конфиденциальности и доступности возможны, то это приведет также к реализации угрозы сохранности информации.

На ***втором этапе*** определяют негативные последствия, которые могут наступить вследствие реализации угроз безопасности информации и оценивают приемлемость ущерба вследствие их наступления.

Вернемся к рассмотренному выше примеру. По результатам первого этапа оценки угроз установлена возможность реализации угроз конфиденциальности и доступности информации для заданного объекта. Негативным последствием реализации угрозы конфиденциальности является разглашение сведений, которые содержаться на рассматриваемом носителе, так как они относятся к информации распространение и (или) предоставление которой ограничено и поэтому такой ущерб не является приемлемым.

Реализация угрозы доступности приведет к не возможности воспользоваться данным документом, но так как есть еще один, схожий по содержанию, то ущерб от этой угрозы приемлем. Исходя из выше указанного, так как ущерб от реализации угрозы конфиденциальности не приемлем, то и от реализации угрозы сохранности (см. определение) информации так же будет не приемлем и поэтому его нужно минимизировать.

На ***третьем этапе*** выбирают методы и средства защиты, которые позволят минимизировать ущерб.

Закончим рассмотрение примера. На втором этапе было определено, что ущерб от угроз конфиденциальности и сохранности не приемлем. Так как возникновение угрозы сохранности обусловлено возникновением угрозы конфиденциальности, то решая проблему конфиденциальности информации можно решить и проблему ее сохранности. Минимизация ущерба может быть реализована за счет того что мы ограничим доступ к бумажному носителю информации. Для этого его нужно со стола переместить в более надежное место, например в сейф. В данном случае сейф будет являться средством защиты информации. Метод, который реализуется – технический, так как сейф – техническое средство.

Как известно, безопасность информации требует комплексного решения проблемы. Поэтому для реализации правовых методов можно предложить разработку инструкции по работе с информацией на бумажных носителях распространение и (или) предоставление которой ограничено. Эта инструкция будет определять порядок работы с бумажными носителями, для того чтобы минимизировать несанкционированный доступ к ним. В качестве организационных мероприятий необходимо обеспечить регулярную проверку (например, раз в неделю или месяц) выполнения положений этой инструкции.

По результатам оценки угроз безопасности информации оформляется таблица 1.

Таблица 1 – Анализ угроз для информационного объекта

Краткое описание защищаемого объекта	Угроза безопасности информации / вид угрозы безопасности информации	Возможные негативные последствия вследствие реализации угрозы	Ущерб (в случае приемлемости указать почему)	Метод защиты	Средство защиты или мероприятие
Информация в виде рукописного текста на бумажном носителе	Физический доступ к носителю информации / Угроза конфиденциальности информации, угроза сохранности информации	Разглашение информации	Не приемлем	Технический	Сейф
				Организационный	Контроль соблюдения инструкции
				Правовой	Инструкция по работе с бумажными документами
	Физический доступ к носителю информации / Угроза доступности информации	Уничтожение информации	Приемлем (есть носитель с аналогичной информацией)		

2 Практическое задание

Необходимо записать в таблицу 2 минимально 5 названий уникальных неповторяющихся угроз безопасности информации для каждого следующего информационного объекта:

– карта флеш памяти с разъемом USB, которая содержит информацию распространение и (или) предоставление которой ограниченно. Устройство хранится на столе. Информация, записанная на устройстве, больше нигде не продублирована;

– персональный компьютер, подключенный к сети Интернет. На компьютере хранится информация распространение и (или) предоставление которой ограничено. В информационной сети на сервере содержится резервная копия этой информации. Компьютер стоит на столе в помещении;

– банковская карта, хранящаяся в тумбочке ее владельца. Карта выпущена в одном экземпляре.

Таблица 2 – Анализ угроз для заданных информационных объектов

Краткое описание защищаемого объекта	Угроза безопасности информации / вид угрозы безопасности информации	Возможные негативные последствия вследствие реализации угрозы	Ущерб (в случае приемлемости указать почему)	Метод защиты	Средство защиты или мероприятие

3 Содержание отчета

3.1 Титульный лист.

3.2 Цель занятия.

3.3 Таблица с результатами анализа угроз безопасности для указанных в практическом задании информационных объектов.