Как узнать – откуда напасть
или
откуда исходит угроза безопасности информации

С. В. Вихорев, директор департамента ОАО «Элвис Плюс»
Р. Ю. Кобцев, менеджер ОАО «Элвис Плюс»

«Чуть опасность где видна,
Верный сторож как со сна
Шевельнется, встрепенется,
К той сторонке обернется…»
А.С. Пушкин «Сказка о золотом Петушке»

К тому, что мало-мальски солидная защита информации должна носить комплексный характер, люди начинают постепенно привыкать. Все больше компаний пропагандируют свои решения в области обеспечения информационной безопасности как комплексные. Организация обеспечения безопасности информации должна не просто носить комплексный характер, но еще и основываться на глубоком анализе возможных негативных последствий. При этом важно не упустить какие-либо существенные аспекты. Все больше в прошлое уходит бесполезное нагромождение различных средств защиты, которое стало «модным» в результате реакции на первую волну страха перед компьютерными преступлениями.

Компании заказчики больше не хотят выбрасывать деньги на ветер, они хотят покупать только то, что им действительно необходимо для построения надежной системы защиты информации и при этом с минимальными расходами на это. И на это они имеют полное как моральное, так и, что более весомо, экономическое право. А то, что стрелять из пушки по воробьям так же бесполезно, как и бросаться с пистолетом на танк, это, думаем, объяснять не надо. А чтобы этого не было, необходимо знать о характере возможных опасностей, чтобы подготовить адекватные средства защиты от них. Поэтому мы и начали эту статью с такого, казалось бы, нелепого эпиграфа – знание источника опасности решает половину дела (кто не помнит, может перечитать сказку). То же самое и в области защиты информации. На пример, нужно ли на компьютер руководителя организации нагромождать кучу средств защиты от НСД, если он и в отдельном кабинете стоит, и на огромный замок кабинет закрыт, и вокруг кабинета часовые с собаками? Поэтому на необходимости изучения опасностей, прежде чем принимать меры по защите от них, по нашему мнению, нет необходимости более задерживаться.

А вот о том, как изучать те самые опасности, поговорить не мешало бы. Потому что изучать их тоже можно по-разному. Можно, например, с криком «Ура» броситься на все грабли сразу, и затем каждую новую «шишку на лбу» «заклеивать» новыми сканерами, межсетевыми экранами и VPN-ами (средства, как вы понимаете, выбраны абстрактно). В результате вы получаете надежную, проверенную защиту, с которой ваш бизнес может спать спокойно, если, конечно, после всех напастей у вас еще останутся средства на продолжение экономической деятельности. Можно, конечно, попробовать учиться на чужих ошибках. Но тут положение еще более гиблое. Во-первых, учиться на чужих ошибках у нашего народа вообще не принято – нам бы самим себе создать трудности, мужественно их преодолеть, а затем гордиться этим. А во-вторых, кто ж про свои ошибки расскажет? Ибо нет милей сердцу картины, чем вид соседа в той же самой яме, из которой ты только что сам выбрался.

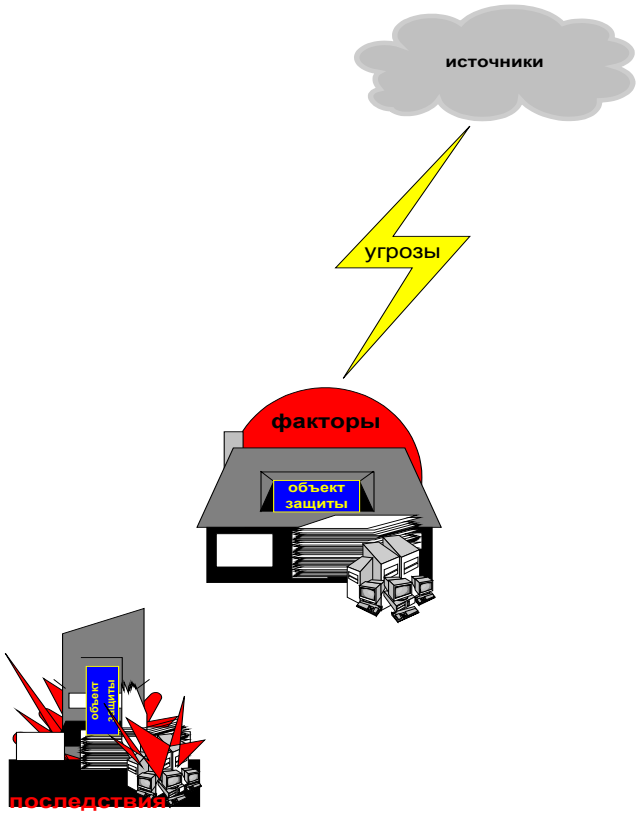
Остается только сначала представить все возможные варианты, а затем отобрать наиболее применимые к конкретному случаю. И как пример можно привести тот факт, что в США только после трагических событий 11 сентября 2001года, когда террористами были захвачены прямо в воздухе сразу несколько рейсов, в гражданских самолетах стали ставить бронированные двери в кабины пилотов, в то время как в СССР такую угрозу предвидели еще на заре гражданской авиации.

Однако пора определиться, что ж все-таки и от чего мы собираемся предостерегать.

И начнем с аксиомы – глупо полагать, что средства защиты информации покупают для того, чтобы поддержать производителей средств защиты. Эгоизм правит миром, и поэтому вся деятельность всех организаций по обеспечению информационной безопасности направлена только на то, чтобы не допустить убытков от потери конфиденциальной информации. Соответственно, этим мы уже предполагаем наличие ценной информации, из-за потери которой компания может понести убытки. А если есть ценная информация то конечно же есть возможность совершения каких-либо действий, которые могут нанести вред этой информации. Все вредоносные действия могут быть совершены только при наличие каких-нибудь слабых мест (уязвимостей), ведь если, к примеру, кто-нибудь захочет проникнуть за кирпичную стену и будет биться в нее головой, то скорее всего у него ничего не получится, однако наличие в стене деревянной калитки уже значительно повышает шансы на успех его героических попыток. И уж конечно если есть действия, то конечно есть нависшая угроза их совершения, а также наличие источников, из которых эти угрозы могут исходить.

И вот благодаря нехитрым логически измышлениям в стиле Вини-Пуха мы получаем цепочку:

источник угрозы – фактор (уязвимость) – угроза (действие) – последствия (атака).



И под этими терминами мы будем понимать:

Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Угроза (действие) [Threat]– это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Фактор (уязвимость) [Vulnerability]– это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Последствия (атака) – это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Как видно из определения, атака – это всегда пара «источник – фактор», реализующая угрозу и приводящая к ущербу.

Попробуем разобраться на абстрактном примере. Вот, предположим, человек ходит на работу каждый день через стройку. И однажды на него падает кирпич, причинив ему при этом ущерб, при котором он теряет трудоспособность и соответственно несет убытки. Попробуем проанализировать данную ситуацию для того, чтобы выявить, что необходимо проанализировать и предусмотреть, чтобы предотвратить ее. Последствия в данном случае – это убытки, которые человек понес в результате несчастного случая. Угрозой у нас выступает кирпич, который упал на человека. Факторами явились то, что путь человека пролегает через стройку, что тропинка на стройке идет прямо под строящимся домом, что с краю на крыше строящегося дома лежит груда кирпичей, что на крышу может пройти кто угодно и т.д. А источником в данной ситуации явилась та некая сила, которая толкнула кирпич – человек, ветер, землетрясение – все эти источники в равной мере могли дать толчок кирпичу, чтобы он полетел вниз. Дальше мы будем постоянно возвращаться к данному примеру, чтобы на нем показать возможность анализа источников угроз и выбора методов парирования.

Если с кирпичами все понятно, то с информацией не на много сложнее. Угроз безопасности информации не так уж и много. Угроза, как следует из определения, это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

1. Ущерб как категория классификации угроз

Проявления возможного ущерба могут быть различны:

- моральный и материальный ущерб деловой репутации организации;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации деятельности организации;
- материальный и моральный ущерб от нарушения международных отношений.

Вот, к примеру, в нашем абстрактном случае с кирпичом на лицо как моральный (испуг, болевой шок и т.д.), так и материальный ущерб (затраты на лечение, длительная нетрудоспособность, возможность потери работы и т.д.).

Однако, стоит заметить, что ущерб может быть причинен как каким-либо субъектом и в этом случае имеется на лицо правонарушение, так и явиться следствием независящим от субъекта проявлений (например, стихийных случаев или иных воздействий, таких как проявления техногенных свойств цивилизации). В первом случае налицо вина[1] субъекта, которая определяет причиненный вред как состав преступления, совершенное по злому умыслу (умышленно, то есть деяние совершенное с прямым или косвенным умыслом[2]) или по неосторожности (деяние, совершенное по легкомыслию, небрежности[3], в результате невиновного причинения вреда[4]) и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом.

Во втором случае ущерб носит вероятностный характер и должен быть сопоставлен, как минимум с тем риском, который оговаривается гражданским, административным или арбитражным правом, как предмет рассмотрения. И определение того, кто именно явился причиной ущерба является вторым по важности (после попытки этого не допустить) вопросом для потерпевшего, потому что дает несчастному ответ на пресловутый вопрос «Кто за все заплатит?»

В теории права под ущербом понимается невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. Ущерб выражается в уменьшении имущества, либо в недополучении дохода, который был бы получен при отсутствии правонарушения (упущенная выгода). То есть, если бы наша жертва падающих кирпичей, спешила на собеседование по устройству на очень выгодную и высокооплачиваемую работу.

При рассмотрении в качестве субъекта, причинившего ущерб какую-либо личность, категория «ущерб» справедлива только в том случае, когда можно доказать, что он причинен, то есть деяния личности необходимо квалифицировать в терминах правовых актов, как состав преступления. Поэтому, при классификации угроз безопасности информации в этом случае целесообразно учитывать требования действующего уголовного права, определяющего состав преступления. Поэтому не будем изобретать велосипед и, как говаривали в старые добрые времена, «обратимся к Марксу»:

Вот некоторые примеры составов преступления, определяемых Уголовным Кодексом Российской Федерации.

Хищение – совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества[5].

Копирование компьютерной информации – повторение и устойчивое запечатление информации на машинном или ином носителе[6].

Уничтожение – внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота[7].

Уничтожение компьютерной информации – стирание ее в памяти ЭВМ[8].

---

[1] УК РФ, 1996 год, ст. 24
[2] УК РФ, 1996 год, ст. 25
[3] УК РФ, 1996 год, ст. 26
[4] УК РФ, 1996 год, ст. 28
[5] УК РФ, 1996 год, ст. 158, примечание 1
[6] УК РФ, 1996 год, ст. 272
[7] УК РФ, 1996 год, ст. 167
[8] УК РФ, 1996 год, ст. 272

Повреждение – изменение свойств имущества при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования[9].

Модификация компьютерной информации – внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных[10].

Блокирование компьютерной информации – искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением[11].

Несанкционированное уничтожение, блокирование модификация, копирование информации – любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией[12].

Обман (отрицание подлинности, навязывание ложной информации) – умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений[13].

Однако, как бы нам порой не хотелось свалить все на природу, говорить о злом умысле личности в уничтожении информации в результате стихийных бедствий не приходится, как и тот факт, что вряд ли стихия сможет воспользоваться конфиденциальной информацией для извлечения собственной выгоды. Хотя и в том и в другом случае собственнику информации причинен ущерб. Здесь правомочно применение категории «причинение вреда имуществу». При этом, речь пойдет не об уголовной ответственности за уничтожение или повреждение чужого имущества, а о случаях подпадающих под гражданское право в части возмещения причиненного ущерба (риск случайной гибели имущества – то есть риск возможного нанесения убытков в связи с гибелью или порчей имущества по причинам, не зависящим от субъектов[14]). По общему правилу в этом случае убытки в связи с гибелью или порчей имущества несет собственник, однако, гражданское право предусматривает и другие варианты компенсации причиненного ущерба.

При рассмотрении в качестве субъекта, причинившего ущерб какое-либо природное или техногенное явление, под ущербом можно понимать невыгодные для собственника имущественные последствия, вызванные этими явлениями и которые могут быть компенсированы за счет средств третьей стороны (страхование рисков наступления события) или за счет собственных средств собственника информации.

Например, страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов[15]. Объектами страхования могут быть не противоречащие законодательству Российской Федерации имущественные интересы связанные с возмещением страхователем причиненного им вреда личности или имуществу физического лица, а также вреда, причиненного юридическому лицу[16]. В общем, как говорил барон Мюнхгаузен, безвыходных ситуаций не бывает – в любом случае можно что-нибудь предусмотреть.

---

[9] УК РФ, 1996 год, ст. 167
[10] УК РФ, 1996 год, ст. 272
[11] УК РФ, 1996 год, ст. 272
[12] УК РФ, 1996 год, ст. 273
[13] Бюллетень Верховного Суда РСФСР, 1982 год, № 2, С.14
[14] Румянцев О. Г., Додонов В.Н., Юридический энциклопедический словарь, М., 1997 г., изд. «ИНФРА-М»
[15] Закон РФ «Об организации страхового дела в Российской Федерации», № 4015-1от 27.10.97 г., ст. 2
[16] Закон РФ «Об организации страхового дела в Российской Федерации», № 4015-1от 27.10.97 г., ст. 4

2. Классификация угроз информационной безопасности

Обобщая изложенное, можно утверждать, что угрозами безопасности информации являются при обеспечении:

- конфиденциальности
  - хищение (копирование) информации и средств ее обработки
  - утрата (неумышленная потеря, утечка) информации и средств ее обработки
- доступности
  - блокирование информации
  - уничтожение информации и средств ее обработки
- целостности
  - модификация (искажение) информации
  - отрицание подлинности информации
  - навязывание ложной информации

3. Классификация источников угроз

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации – внутренние источники, так и вне ее – внешние источники. Деление источников на субъективные и объективные оправдано исходя из предыдущих рассуждений по поводу вины или риска ущерба информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными.

И для наглядности давайте опять прибегнем к нашему примеру. Многие, как это ни странно увидели источник угрозы в стопке кирпичей так неудачно сложенной на крыше. Но ведь падение кирпича явилось в нашем случае всего лишь действием, которое нанесло ущерб. А источником послужила та сила, которая заставила кирпич сорваться вниз. Силой же мог выступить и рабочий, который **случайно** задел стопку кирпичей; это мог быть наемный убийца, который **умышленно** столкнул кирпич; кирпич мог задеть и качающийся на ветру незакрепленный крюк подъемного крана; он мог упасть, в конце концов, из-за внезапного землетрясения.

Итак, получается, что все источники угроз безопасности информации можно разделить на три основные группы:

I. Обусловленные действиями субъекта (антропогенные источники угроз).
II. Обусловленные техническими средствами (техногенные источники угрозы).
III. Обусловленные стихийными источниками.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорит о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние [I.A.], так и внут-

ренние [I.B.]. Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети.

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Обобщая вышесказанное и возвращаясь к нашему примеру, можно сказать, что говоря об антропогенных источниках, речь идет именно о том человеке, который мог скинуть пресловутый кирпич – рабочий стройки, наемный убийца, маньяк и.т.д.

Квалификация антропогенных источников информации играют важную роль в оценке их влияния и учитывается при ранжировании источников угроз.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Помните у Юлиана Семенова в «Семнадцать мгновений весны»: «…Этих идиотов погубит их же техника». Человечество действительно становится все больше зависимо от техники и источники угроз, которые напрямую зависят от свойств техники менее прогнозируемые и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием используемого оборудования, а также отсутствием материальных средств на его обновление. Технические средства, являющиеся источниками потенциальных угроз безопасности информации так же могут быть внешними [II.A.] и внутренними [II.B.].

Возвращаясь к примеру, на котором мы решили упрощенно показать все стороны дела, можно заметить, что даже в нашем, совсем не техническом случае можно найти множество техногенных источников: незакрепленный болтающийся на ветру крюк подъемного крана, брошенная на крыше тачка из под цемента, которая могла покатиться и т.д. А что уж говорить про информационные системы, которые полностью основаны на различной технике, гораздо более сложной чем подъемный кран или тачка.

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе[17] в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда. Хотя, конечно, если предположить, что в нашем примере кирпич бросил домовой, то спрогнозировать эту ситуацию сложно, а вот если дом стоит в месте, где постоянно происходят землетрясения, то стройку лучше обойти стороной.

[17] Румянцев О. Г., Додонов В.Н., Юридический энциклопедический словарь, М., 1997 г., изд. «ИНФРА-М»

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы [III.A.].

Классификация и Перечень источников угроз приведен в Таблице.

Классификация и перечень источников угроз информационной безопасности

	Источники угроз информационной безопасности
[I.0.0]	*АНТРОПОГЕННЫЕ ИНСТОЧНИКИ*
[I.A.0]	***Внешние антропогенные источники***
[I.A.1]	криминальные структуры
[I.A.2]	потенциальные преступники и хакеры
[I.A.3]	недобросовестные партнеры
[I.A.4]	технический персонал поставщиков телематических услуг
[I.A.5]	представители надзорных организаций и аварийных служб
[I.A.6]	представители силовых структур
[I.B.0]	***Внутренние антропогенные источники*)***
[I.B.1]	основной персонал (пользователи, программисты, разработчики)
[I.B.2]	представители службы защиты информации (администраторы)
[I.B.3]	вспомогательный персонал (уборщики, охрана)
[I.B.4]	технический персонал (жизнеобеспечение, эксплуатация)
[II.0.0]	*ТЕХНОГЕННЫЕ ИСТОЧНИКИ*
[II.A.0]	***Внешние техногенные источники угроз***
[II.A.1]	средства связи
[II.A.2]	сети инженерных коммуникации (водоснабжения, канализации)
[II.A.3]	транспорт
[II.B.0]	***Внутренние техногенные источники угроз***
[II.B.1]	некачественные технические средства обработки информации
[II.B.2]	некачественные программные средства обработки информации
[II.B.3]	вспомогательные средства (охраны, сигнализации, телефонии)
[II.B.4]	другие технические средства, применяемые в учреждении
[III.0.0]	*СТИХИЙНЫЕ ИСТОЧНИКИ УГРОЗ*
[III.A.0]	***Внешние стихийные источники***
[III.A.1]	пожары
[III.A.2]	землетрясения
[III.A.3]	наводнения
[III.A.4]	ураганы
[III.A.5]	магнитные бури
[III.A.6]	радиоактивное излучение
[III.A.7]	различные непредвиденные обстоятельства
[III.A.8]	необъяснимые явления
[III.A.9]	другие форс-мажорные обстоятельства**)

Примечания:*) Особую группу внутренних антропогенных источников составляют специально внедренные и завербованные агенты из числа основного, вспомогательного, технического персонала и представителей службы защиты информации. Эта группа не рассматривается как самостоятельная, но при анализе, в случае возникновения потенциальной возможности внедрения агентов, необходимо учитывать особенности защиты от таких источников при рассмотрении возможностей внутренних антропогенных источников.

**) В данном случае под термином «другие форс-мажорные обстоятельства» понимается юридическая составляющая форс-мажора, то есть различные решения высших государственных органов, забастовки, войны, революции и т. п., приводящие к возникновению обстоятельств непреодолимой силы.

Ранжирование источников угроз

При выборе метода ранжирования источников угроз использовалась методология, изложенная в международных стандартах[18], а также практический опыт российских экспертов в области информационной безопасности.

Все источники угроз имеют разную степень опасности $(К_{оп})_i$, которую можно количественно оценить, проведя их ранжирование. При этом, оценка степени опасности проводится по косвенным показателям. В качестве критериев сравнения (показателей) можно, к примеру, выбрать:

- **Возможность возникновения источника $(К_1)_i$** – определяет степень доступности к возможности использовать фактор (уязвимость) (для антропогенных источников) (например, охраняется или нет стройка, есть ли лестница на крышу и т.д.), удаленность от фактора (уязвимости) (для техногенных источников) (например, на каком расстоянии от стопки кирпичей находится крюк подъемного крана и т.д.) или особенности обстановки (для случайных источников) (например, сейсмическая обстановка).
- **Готовность источника $(К_2)_i$** – определяет степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников) (например, простой строитель или профессиональный убийца, а также жертва - бедный человек или же он наследник крупного наследства и т.д.), или наличие необходимых условий (для техногенных и стихийных источников) (например, закреплен или нет крюк подъемного крана, есть ветер или нет, который может его раскачать, есть ли прогноз на землетрясение и т.д.).
- **Фатальность $(К_3)_i$** – определяет степень неустранимости последствий реализации угрозы (например, лежит ли стопка кирпичей на крыше или же над тропинкой висит бетонная плита и т.д.).

Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе. Причем, 1 соответствует самой минимальной степени влияния оцениваемого показателя на опасность использования источника, а 5 – максимальной.

$(К_{оп})_i$ для отдельного источника можно определить как отношение произведения вышеприведенных показателей к максимальному значению (125).

$$(К_{оп})_i = \frac{(К_1 * К_2 * К_3)}{125}$$

Степень доступности к защищаемому объекту может быть классифицирована по следующей шкале:

- высокая степень доступности – антропогенный источник угроз имеет полный доступ к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников, наделенных максимальными правами доступа, например, представители служб безопасности информации, администраторы);
- первая средняя степень доступности – антропогенный источник угроз имеет возможность опосредованного, не определенного функциональными обязанностями, (за счет побочных каналов утечки информации, использования возможности доступа к привилегированным рабочим местам) доступа к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников);

[18] Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 «Практические правила управления информационной безопасностью»)

- вторая средняя степень доступности – антропогенный источник угроз имеет ограниченную возможность доступа к программным средствам в силу введенных ограничений в использовании технических средств, функциональных обязанностей или по роду своей деятельности (характерно для внутренних антропогенных источников с обычными правами доступа, например, пользователи, или внешних антропогенных источников, имеющих право доступа к средствам обработки и передачи защищаемой информации, например, хакеры, технический персонал поставщиков телематических услуг);
- низкая степень доступности – антропогенный источник угроз имеет очень ограниченную возможность доступа к техническим средствам и программам, обрабатывающим защищаемую информацию (характерно для внешних антропогенных источников).
- отсутствие доступности – антропогенный источник угроз не имеет доступа к техническим средствам и программам, обрабатывающих защищаемую информацию.

Степень удаленности от защищаемого объекта можно характеризовать следующими параметрами:

- совпадающие объекты – объекты защиты сами содержат источники техногенных угроз и их территориальное разделение невозможно;
- близко расположенные объекты – объекты защиты расположены в непосредственной близости от источников техногенных угроз и любое проявление таких угроз может оказать существенное влияние на защищаемый объект;
- средне удаленные объекты – объекты защиты располагаются на удалении от источников техногенных угроз, на котором проявление влияния этих угроз может оказать не существенное влияние на объект защиты;
- удаленно расположенные объекты – объект защиты располагается на удалении от источника техногенных угроз, исключающем возможность его прямого воздействия.
- сильно удаленные объекты – объект защиты располагается на значительном удалении от источников техногенных угроз, полностью исключающем любые воздействия на защищаемый объект, в том числе и по вторичным проявлениям.

Особенности обстановки характеризуются расположением объектов защиты в различных природных, климатических, сейсмологических, гидрологических и других условиях. Особенности обстановки можно оценить по следующей шкале:

- очень опасные условия – объект защиты расположен в зоне действия природных катаклизмов;
- опасные условия – объект защиты расположен в зоне, в которой многолетние наблюдения показывают возможность проявления природных катаклизмов;
- умеренно опасные условия – объект защиты расположен в зоне в которой по проводимым наблюдениям на протяжении долгого периода отсутствуют проявления природных катаклизмов, но имеются предпосылки возникновения стихийных источников угроз на самом объекте;
- слабо опасные условия – объект защиты находится вне пределов зоны действия природных катаклизмов, однако на объекте имеются предпосылки возникновения стихийных источников угроз;
- неопасные условия – объект защиты находится вне пределов зоны действия природных катаклизмов и на объекте отсутствуют предпосылки возникновения стихийных источников угроз.

Квалификация антропогенных источников играет важную роль в определении их возможностей по совершению противоправных деяний. Принята следующая классификация уровня квалификации по возможности (уровню) взаимодействия с защищаемой сетью[19]:

- нулевой уровень – определяется отсутствием возможности какого-либо использования программ;
- первый уровень – ограничивается возможностью запуска задач/программ из фиксированного набора, предназначенного для обработки защищаемой информации (уровень неквалифицированного пользователя);
- второй уровень – учитывает возможность создания и запуска пользователем собственных программ с новыми функциями по обработке информации (уровень квалифицированного пользователя, программиста);
- третий уровень – определяется возможностью управления функционированием сетью, то есть воздействием на базовое программное обеспечение, ее состав и конфигурацию (уровень системного администратора);
- четвертый уровень – определяется всем объемом возможностей субъектов, осуществляющих проектирование и ремонт технических средств, вплоть до включения в состав сети собственных технических средств с новыми функциями по обработке информации (уровень разработчика и администратора).

Нулевой уровень является самым низким уровнем возможностей по ведению диалога источника угроз с защищаемой сетью. При оценке возможностей антропогенных источников предполагается, что субъект, совершающий противоправные действия, либо обладает, либо может воспользоваться правами соответствующего уровня.

Привлекательность совершения деяния со стороны источника угроз устанавливается следующим образом:

- особо привлекательный уровень – защищаемые информационные ресурсы содержат информацию, которая может нанести непоправимый урон и привести к краху организации, осуществляющей защиту;
- привлекательный уровень – защищаемые информационные ресурсы содержат информацию, которая может быть использована для получения выгоды в пользу источника угрозы или третьих лиц;
- умеренно привлекательный уровень – защищаемые информационные ресурсы, содержат информацию, разглашение которой может нанести ущерб отдельным личностям;
- слабо привлекательный уровень – защищаемые информационные ресурсы содержат информацию, которая при ее накоплении и обобщении в течение определенного периода может причинить ущерб организации, осуществляющей защиту;
- не привлекательный уровень – информация не представляет интерес для источника угрозы.

Необходимые условия готовности источника определяются исходя из возможности реализации той или иной угрозы в конкретных условиях расположения объекта. При этом предполагается:

- угроза реализуема – то есть условия благоприятны или могут быть благоприятны для реализации угрозы (например, активизация сейсмической активности);

[19] Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», Гостехкомиссия России, Сборник руководящих документов по защите информации от несанкционированного доступа, М., 1998 г., п. 4

- угроза умеренно реализуема – то есть условия благоприятны для реализации угрозы, однако долгосрочные наблюдения не предполагают возможности ее активизации в период существования и активной деятельности объекта защиты;
- угроза слабо реализуема – то есть существуют объективные причины на самом объекте или в его окружении, препятствующие реализации угрозы;
- угроза не реализуема – то есть отсутствуют предпосылки для реализации предполагаемого события.

Степень неустранимости последствий проявления угрозы (фатальность) определяется по следующей шкале:

- неустранимые последствия – результаты проявления угрозы могут привести к полному разрушению (уничтожению, потере) объекта защиты, как следствие к невосполнимым потерям и исключению возможности доступа к защищаемым информационным ресурсам;
- практически неустранимые последствия – результаты проявления угрозы могут привести к разрушению (уничтожению, потере) объекта и к значительным затратам (материальным, временным и пр.) на восстановление последствий, сопоставимых с затратами на создание нового объекта и существенному ограничению времени доступа к защищаемым ресурсам;
- частично устранимые последствия – результаты проявления угрозы могут привести к частичному разрушению объекта защиты и, как следствие, к значительным затратам на восстановление, ограничению времени доступа к защищаемым ресурсам;
- устранимые последствия – результаты проявления угрозы могут привести к частичному разрушению (уничтожению, потере) объекта защиты, не требующих больших затрат на его восстановление и, практически не влияющих на ограничение времени доступа к защищаемым информационным ресурсам;
- отсутствие последствий – результаты проявления угрозы не могут повлиять на деятельность объекта защиты.

Результаты проведенного ранжирования относительно конкретного объекта защиты можно свести в таблицу, позволяющую определить наиболее опасные для данного объекта источники угроз безопасности информации.

При выборе допустимого уровня источника угроз. предполагается, что источники угроз, имеющие коэффициент $(К_{оп})_i$ менее (0,1…0,2) могут в дальнейшем не учитываться, как маловероятные.

Определение актуальных (наиболее опасных) угроз осуществляется на основе анализа расположения объектов защиты и структуры построения информационной системы, а также информационных ресурсов, подлежащих защите.

4. Классификация уязвимостей безопасности

А теперь все-таки от абстрактного к конкретному. Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности информации на конкретном объекте информатизации.

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу,

пользователю информации) Кроме того, возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть:

[A] объективными

[B] субъективными

[C] случайными.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации.

Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами.

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности.

Уязвимости можно разделить на классы (обозначены заглавными буквами), группы (обозначены римскими цифрами) и подгруппы (обозначены строчными буквами). Классификация и Перечень уязвимостей информационной безопасности приведен в Таблице .

Классификация и Перечень уязвимостей информационной безопасности

Код	Уязвимости информационной безопасности
[A.0.0.0]	**ОБЪЕКТИВНЫЕ УЯЗВИМОСТИ**
[A.I.0.0]	**сопутствующие техническим средствам излучения**
[A.I.a.0]	*электромагнитные*
[A.I.a.1]	побочные излучения элементов технических средств
[A.I.a.2]	кабельных линий технических средств
[A.I.a.3]	излучения на частотах работы генераторов
[A.I.a.4]	на частотах самовозбуждения усилителей
[A.I.b.0]	*электрические*
[A.I.b.1]	наводки электромагнитных излучений на линии и проводники
[A.I.b.2]	просачивание сигналов в цепи электропитания, в цепи заземления
[A.I.b.3]	неравномерность потребления тока электропитания [3]
[A.I.c.0]	*звуковые*
[A.I.c.1]	акустические
[A.I.c.2]	виброакустические
[A.II.0.0]	**активизируемые**
[A.II.a.0]	*аппаратные закладки устанавливаемые*
[A.II.a.1]	в телефонные линии
[A.II.a.2]	в сети электропитания
[A.II.a.3]	в помещениях
[A.II.a.4]	в технических средствах
[A.II.b.0]	*программные закладки*
[A.II.b.1]	вредоносные программы
[A.II.b.2]	технологические выходы из программ
[A.II.b.3]	нелегальные копии ПО

[A.III.0.0]	**определяемые особенностями элементов**
[A.III.a.0]	*элементы, обладающие электроакустическими преобразованиями*
[A.III.a.1]	телефонные аппараты
[A.III.a.2]	громкоговорители и микрофоны
[A.III.a.3]	катушки индуктивности
[A.III.a.4]	дроссели
[A.III.a.5]	трансформаторы и пр.
[A.III.b.0]	*элементы, подверженные воздействию электромагнитного поля*
[A.III.b.1]	магнитные носители
[A.III.b.2]	микросхемы
[A.III.b.3]	нелинейные элементы, подверженные ВЧ навязыванию
[A.IV.0.0]	**определяемые особенностями защищаемого объекта**
[A.IV.a.0]	*местоположением объекта*
[A.IV.a.1]	отсутствие контролируемой зоны
[A.IV.a.2]	наличие прямой видимости объектов
[A.IV.a.3]	удаленных и мобильных элементов объекта
[A.IV.a.4]	вибрирующих отражающих поверхностей
[A.IV.b.0]	*организацией каналов обмена информацией*
[A.IV.b.1]	использование радиоканалов
[A.IV.b.2]	глобальных информационных сетей
[A.IV.b.3]	арендуемых каналов
[B.0.0.0]	**СУБЪЕКТИВНЫЕ УЯЗВИМОСТИ**
[B.I.0.0]	**ошибки (халатность)**
[B.I.a.0]	*при подготовке и использовании программного обеспечения*
[B.I.a.1]	при разработке алгоритмов и программного обеспечения
[B.I.a.2]	при инсталляции и загрузке программного обеспечения
[B.I.a.3]	при эксплуатации программного обеспечения
[B.I.a.4]	при вводе данных (информации)
[B.I.a.5]	при настройке сервисов универсальных систем
[B.I.a.6]	самообучающейся (самонастраивающейся) сложной системы систем
[B.I.b.0]	*при эксплуатации технических средств*
[B.I.b.1]	при включении/выключении технических средств
[B.I.b.2]	при использовании технических средств охраны
[B.I.b.3]	при использовании средств обмена информацией
[B.I.c.0]	*некомпетентные действия*
[B.I.c.1]	при конфигурировании и управлении сложной системы
[B.I.c.2]	при настройке программного обеспечения
[B.I.c.3]	при организации управления потоками обмена информации
[B.I.c.4]	при настройке технических средств
[B.I.c.5]	при настройке штатных средств защиты программного обеспечения
[B.I.d.0]	*неумышленные действия*
[B.I.d.1]	повреждение (удаление) программного обеспечения
[B.I.d.2]	повреждение (удаление) данных
[B.I.d.3]	повреждение (уничтожение) носителей информации
[B.I.d.4]	повреждение каналов связи
[B.II.0.0]	**нарушения**
[B.II.a.0]	*режима охраны и защиты*
[B.II.a.1]	доступа на объект
[B.II.a.2]	доступа к техническим средствам
[B.II.a.3]	соблюдения конфиденциальности
[B.II.b.0]	*режима эксплуатации технических средств и ПО*
[B.II.b.1]	энергообеспечения
[B.II.b.2]	жизнеобеспечения
[B.II.b.3]	установки нештатного оборудования
[B.II.b.4]	инсталляции нештатного ПО (игрового, обучающего, технологического)
[B.II.c.0]	*использования информации*
[B.II.c.1]	обработки и обмена информацией
[B.II.c.2]	хранения и уничтожения носителей информации
[B.II.c.3]	уничтожения производственных отходов и брака
[B.III.0.0]	**психогенные**
[B.III.a.0]	*психологические*

[B.III.a.1]	антагонистические отношения (зависть, озлобленность, обида)
[B.III.a.3]	неудовлетворенность своим положением
[B.III.a.4]	неудовлетворенность действиями руководства (взыскание, увольнение)
[B.III.a.5]	психологическая несовместимость
[B.III.b.0]	*психические*
[B.III.b.1]	психические отклонения
[B.III.b.2]	стрессовые ситуации
[B.III.c.0]	*физиологические*
[B.III.c.1]	физическое состояние (усталость, болезненное состояние)
[B.III.c.2]	психосоматическое состояние
[C.0.0.0]	**СЛУЧАЙНЫЕ УЯЗВИМОСТИ**
[C.I.0.0]	**сбои и отказы**
[C.I.a.0]	*отказы и неисправности технических средств*
[C.I.a.1]	обрабатывающих информацию
[C.I.a.2]	обеспечивающих работоспособность средств обработки информации
[C.I.a.3]	обеспечивающих охрану и контроль доступа
[C.I.b.0]	*старение и размагничивание носителей информации*
[C.I.b.1]	дискет и съемных носителей
[C.I.b.2]	жестких дисков
[C.I.b.3]	элементов микросхем
[C.I.b.4]	кабелей и соединительных линий
[C.I.c.0]	*сбои программного обеспечения*
[C.I.c.1]	операционных систем и СУБД
[C.I.c.2]	прикладных программ
[C.I.c.3]	сервисных программ
[C.I.c.4]	антивирусных программ
[C.I.d.0]	*сбои электроснабжения*
[C.I.d.1]	оборудования, обрабатывающего информацию
[C.I.d.2]	обеспечивающего и вспомогательного оборудования

Ранжирование уязвимостей

Все уязвимости имеют разную степень опасности $(К_{оп})_f$, которую можно количественно оценить, проведя их ранжирование. При этом, в качестве критериев сравнения (показателей) можно выбрать:

- **Фатальность** $(К_1)_f$ – определяет степень влияния уязвимости на неустранимость последствий реализации угрозы. Для объективных уязвимостей это **Информативность** – способность уязвимости полностью (без искажений) передать полезный информационный сигнал.
- **Доступность** $(К_2)_f$ – определяет удобство (возможность) использования уязвимости источником угроз (массогабаритные размеры, сложность, стоимость необходимых средств, возможность использования не специализированной аппаратуры).
- **Количество** $(К_3)_f$ – определяет количество элементов объекта, которым характерен та или иная уязвимость.

$(К_{оп})_f$ для отдельной уязвимости можно определить как отношение произведения вышеприведенных показателей к максимальному значению (125).

$$(К_{оп})_f = \frac{(К_1 * К_2 * К_3)}{125}$$

Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе. Причем, 1 соответствует самой минимальной степени влияния оцениваемого показателя на опасность использования уязвимости, а 5 – максимальной.

Для подгруппы уязвимостей $^{пг}(К_{оп})_f$ определяется как среднее арифметическое коэффициентов отдельных уязвимостей в подгруппе.

Для удобства анализа, $^{г}(К_{оп})_f$ для группы нормируется относительно совокупности всех коэффициентов подгрупп в своем классе, а $^{к}(К_{оп})_f$ для класса определяется как совокупность коэффициентов подгрупп класса нормированных относительно всей совокупности коэффициентов подгрупп.

Результаты анализа с указанием коэффициентов опасности каждой уязвимости, сводятся в таблицу.

5. Классификация актуальных угроз

При определении актуальных угроз, экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

Поэтому, возвращаясь к примеру, если на заброшенной неохраняемой стройке прямо над тропинкой на старом подъемном кране висит огромная бетонная плита, а у вас в кармане миллион – то тут, по всем коэффициентам, как говорится, «туда не ходи, сюда ходи, а то снег башка попадет – совсем мертвый будешь…» Или по крайней мере необходимо принять меры защиты – обойти опасное место, надеть каску, взять с собой охрану, никому не говорить о миллионе и т.д.

А если не на пример – то на основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей из которой определяются возможные последствия реализации угроз (атаки) и вычисляется коэффициент опасности этих атак как произведение коэффициентов опасности соответствующих угроз и источников угроз, определенных ранее. При этом предполагается, что атаки, имеющие коэффициент опасности менее 0,1 (предположение экспертов), в дальнейшем могут не рассматриваться из-за малой вероятности их совершения на рассматриваемом объекте.

Предложенная классификация может служить основой для выработки методики оценки актуальности той или иной угрозы, а уже по выявлению наиболее актуальных угроз могут приниматься меры по выбору методов и средств для их парирования.

И на последок мы хотели бы сказать, что конечно же все вышесказанное является нашим сугубо субъективным мнением и не является панацеей при построении системы безопасности информации. Однако, как сказал в свое время В.Г. Белинский, найти причину зла - почти тоже, что найти против него лекарство. Вот и мы говорим, что уже сам принцип системного подхода к решению вопросов информационной безопасности позволяет заложить комплекс мероприятий по парированию угроз безопасности информации уже на стадии проектирования защищенной сети, тем самым избавив себя от излишних затрат в дальнейшем.