Содержание

Практическое занятие №1
Методика оценки уязвимости информации

Цель практического занятия работы – закрепление теоретических знаний и практическое освоение методики количественной оценки уязвимости информации.

Время - 4 часа.

1. Основные теоретические сведения

При решении широкого круга практических задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости. В лабораторной работе рассматривается один из возможных подходов к определению этой оценки.

Несанкционированное получение информации в телекоммуникационной системе (ТКС) возможно не только путем непосредственного доступа к базам данных, но и многими другими путями, не требующими такого доступа. При этом основную опасность представляют собой преднамеренные действия злоумышленников. Воздействие случайных факторов само по себе не ведет к несанкционированному получению информации, но лишь способствует появлению канала несанкционированного получения информации (КНПИ), которым может воспользоваться злоумышленник.

Территориально потенциально возможные несанкционированные действия могут иметь место в различных зонах [1]:

- внешней зоне – неконтролируемой территории вокруг объектов ТКС, на которой не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации;
- зоне контролируемой территории – территории вокруг объектов ТКС, которая непрерывно контролируется специальными средствами и персоналом;
- зоне помещений – внутреннего пространства помещений, в которых располагаются объекты ТКС;
- зоне ресурсов – части помещений, откуда возможен непосредственный доступ к ресурсам системы;
- зоне баз данных – части ресурсов системы, из которых возможен непосредственный доступ к защищаемым данным.

При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий:

1) нарушитель должен получить доступ в соответствующую зону;
2) во время нахождения нарушителя в зоне в ней должен проявиться соответствующий КНПИ;

3) проявившийся КНПИ должен быть доступен нарушителю соответствующей категории;

4) в КНПИ в момент доступа к нему нарушителя должна находиться защищаемая информация.

В целях получения выражения для показателя уязвимости информации в ТКС введем следующие обозначения [1,2]: $P_{Дikl}$ - вероятность доступа нарушителя k-й категории в l-тую зону i-го компонента ТКС; P_{Kijl} - вероятность проявления j-го КНПИ в l-й зоне i-го компонента ТКС; P_{Hijkl} - вероятность доступности нарушителя k-й категории j-го КНПИ в l-й зоне i-го компонента ТКС при условии доступа нарушителя в зону; $P_{Иijl}$ - вероятность наличия защищаемой информации в j-м КНПИ в l-й зоне i-го компонента ТКС в момент доступа туда нарушителя.

Тогда вероятность несанкционированного получения информации нарушителем k-й категории по j-му КНПИ в l-й зоне i-го компонента ТКС определяется как:

$$P_{kjli} = P_{Дikl} P_{Kijl} P_{Hijkl} P_{Иijl}. \qquad (1)$$

Назовем эту вероятность **базовым показателем уязвимости информации**. Вместе с тем базовые показатели уязвимости, рассчитанные в соответствии с (1), сами по себе имеют ограниченное практическое применение. Для решения задач анализа систем защиты необходимы значения показателей уязвимости, обобщенных по какому либо индексу или их комбинации.

Например, вероятность несанкционированного получения информации в одном компоненте ТКС одним злоумышленником одной категории по одному КНПИ будет иметь вид:

$$P_{kji} = 1 - \prod_{l=1}^{5} (1 - P_{kjli}). \qquad (2)$$

Обобщая это выражение по множеству k получаем вероятность несанкционированного получения информации всем указанным множеством нарушителей:

$$P_{ij} = 1 - \prod_{k=1}^{K} (1 - P_{kji}). \qquad (3)$$

Нетрудно получить и обобщенное выражение для оценки показателя уязвимости ТКС:

$$P_i = 1 - \prod_{j=1}^{J} (1 - P_{ji}), \; P = 1 - \prod_{i=1}^{I} (1 - P_i) \qquad (4)$$

На практике наибольший интерес представляет определение наиболее неблагоприятных условий защищенности ТКС, т.е. определение самого уязвимого структурного компонента системы, самого опасного КНПИ, самой опасной категории нарушителей и т.д.Особенностью рассмотренного подхода оценки уязвимости информации является отсутствие учета интервала времени, на котором оценивается уязвимость.

2. Порядок выполнения практического занятия

При подготовке к практическому занятию

На этапе подготовки к практическому занятию студенты должны, используя литературу [1,2] и материалы лекций углубить свои знания по методам оценки уязвимости информации.

Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.Каждая подгруппа получает от преподавателя индивидуальный вариант задания на практическое занятие, который представляет собой значения вероятностей $P_{Дikl}$, P_{Kijl}, P_{Hijkl}, $P_{Иijl}$ для определения показателей уязвимости.

Студенты должны:

1. Вычислить значения базовых показателей уязвимости информации в соответствии с выражением (1).
2. Используя методику представленную выражениями (2-4) вычислить значения показателей уязвимости. Определить наиболее опасную зону, категорию нарушителя, КНПИ.
3. Определить обобщенное значение показателя уязвимости ТКС.

3. Контрольные вопросы

1. Дайте определения безопасности информации, уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации.Перечислите источники угроз безопасности информации.
2. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
3. Поясните суть методики оценки уязвимости информации.

Литература

1. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 3-е издание. – М.: Горячая линия-Телеком, 2005.

2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов. – М.: Горячая линия-Телеком, 2004.

Практическое занятие №2
Методика расчета показателей помехозащищенности телекоммуникационных систем гражданской авиации

Цель практического занятия – закрепление теоретических знаний в области помехозащищенности телекоммуникационных систем (ТКС) и освоение методики расчета показателей помехозащищенности.

Время - 4 часа.

1. Основные теоретические сведения

Помехозащищенность ТКС представляет собой совокупность способов и средств, обеспечивающих устойчивую работу системы в условиях воздействия на нее как непреднамеренных, так и организованных помех [1]. Помехозащищенность системы связи определяется ее скрытностью и помехоустойчивостью.

Под **скрытностью ТКС** понимается способность этих систем противостоять мерам радиоразведки. Радиоразведка предполагает, как правило, выполнение следующих основных задач [1,2]:

- обнаружение факта работы системы связи (обнаружение сигнала);
- определение структуры обнаруженного сигнала;
- раскрытие содержащейся в сигнале информации;
- пеленгация средств системы связи.

Первые три задачи решаются последовательно и им могут быть противопоставлены три вида скрытности:

- энергетическая скрытность;
- структурная скрытность;
- информационная скрытность.

Энергетическая скрытность характеризует способность противостоять мерам, направленным на обнаружение сигнала разведывательными средствами противника (злоумышленника). Как известно, обнаружение сигнала разведывательным приемником происходит в условиях, когда на его вход действуют помехи, что приводит к ошибкам двух видов: пропуск сигнала при его наличии и ложное обнаружение при отсутствии сигнала (ложная тревога). Эти ошибки носят вероятностный характер. Количественной мерой энергетической скрытности является вероятность правильного обнаружения $P_{обн}$, при заданной вероятности ложной тревоги $P_{лт}$, которая в свою очередь зависит от отношения

сигнал-помеха в рассматриваемой радиолинии и правила принятия решения об обнаружении сигнала.

Структурная скрытность характеризуется способностью противостоять мерам радиотехнической разведки, направленным на раскрытие сигнала. Это означает распознавание формы сигнала, определяемой способами его кодирования и модуляции, т.е. отождествление обнаруженного сигнала с одним из множества априорно известных сигналов. Следовательно, для увеличения структурной скрытности необходимо иметь по возможности больший ансамбль используемых сигналов и достаточно часто менять форму сигналов. Задача определения структуры сигнала является статистической, а количественной мерой структурной скрытности может служить вероятность раскрытия структуры сигнала $P_{стр}$ при условии, что сигнал обнаружен.

Информационная скрытность определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемой с помощью сигнала информации. Раскрытие смысла передаваемой информации означает отождествление каждого принятого сигнала или их совокупности с тем сообщением, которое передается. Наличие априорной и апостериорной неопределенности делает эту задачу вероятностной, а за количественную меру информационной скрытности принимают вероятность раскрытия смысла передаваемой информации $P_{инф}$ при условии, что сигнал обнаружен и выделен.

Скрытность количественно определяется вероятностью разведки сигнала:

$$P_р = P_{обн} P_{стр} P_{инф}. \qquad (1)$$

Достаточно часто задача раскрытия смысла передаваемой информации не ставиться (при организации радиоэлектронного противодействия), и тогда можно принять $P_{инф} = 1$. В ряде случаев для организации радиоэлектронного противодействия достаточно обнаружить сигнал подавляемой системы связи, т.е. $P_{стр} = 1$ и $P_р = P_{обн}$. Таким образом, энергетическая скрытность является важнейшей характеристикой системы связи.

Оценим вероятность обнаружения сигнала $P_{обн}$, зависящую от отношения сигнал-шум q в полосе F линейной части разведывательного приемника:

$$q = 2\frac{P_c}{P_ш} = 2\frac{P_c}{NF} = 2\frac{E}{N_р}, \qquad (2)$$

где P_c, $P_ш$ - мощности сигнала и помехи, соответственно; N - спектральная плотность помехи; энергия реализации процесса $y(t)$ на входе разведприемника за время $t_и$

$$E = \int_0^{t_u} y^2(t)dt\,. \qquad (3)$$

Процесс на входе разведприемника представляет собой аддитивную смесь сигнала $s(t)$ и помехи $n(t)$ или только помеху, при отсутствии сигнала:

$$y(t) = \begin{cases} s(t) + n(t), \\ n(t). \end{cases} \qquad (4)$$

Форма разведуемого сигнала неизвестна, тогда единственным признаком наличия сигнала является энергия (3). Разведприемник содержит, как правило, линейный полосовой фильтр с полосой F, квадратичный детектор, интегратор с постоянной интегрирования t_u и пороговое устройство. Типичная схема линии связи представлена на рис.1.

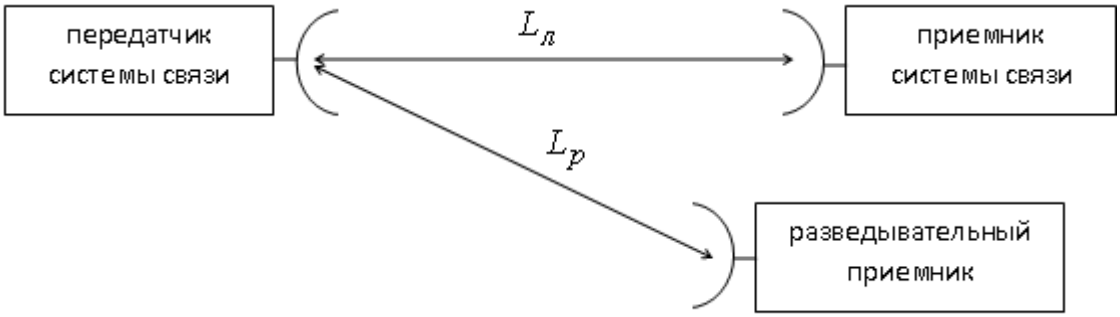

Рис. 1. Схема линии связи с разведприемником

Будем считать, что система связи работает в штатном режиме с заданным качеством при определенном значении $2E_б$, где $E_б$ - энергия на бит информации. Тогда требуемое отношение сигнал-шум:

$$\left(2\frac{P_c}{N}\right)_{тр} = 2\frac{RE_б}{N}, \qquad (5)$$

где $R = \dfrac{1}{T_б}$ - скорость передачи информации, бит/с.

При известной мощности передатчика $P_{прд}$, коэффициентах усиления передающей и приемной антенн $G_{прд}$, $G_{прм}$, затухания в среде до приемника $L_л$, коэффициенте запаса на мощности $k_з$ и шумовой температуре приемника $T_{ш_{прм}}$ имеем:

$$\left(2\frac{P_c}{N}\right)_{тр}=\frac{P_{прд}G_{прд}G_{прм}}{kk_з T_{ш_{прм}} L_л}, \qquad (6)$$

где k - постоянная Больцмана.

Приравнивая правые части выражений (5) и (6) получаем выражение для минимальной мощности передатчика линии связи:

$$P_{прд}=\frac{2kk_з T_{ш_{прм}} RL_л E_б}{G_{прд}G_{прм}N}. \qquad (7)$$

Отношение сигнал-шум на входе разведприемника:

$$\left(2\frac{P_c}{N_p}\right)=\frac{P_{прд}G_{прд_p}G_{прм_p}}{kT_{ш_p}L_p}, \qquad (8)$$

где $G_{прд_p}$ - коэффициент усиления передающей антенны по боковым лепесткам диаграммы направленности; $G_{прм_p}$ - коэффициент усиления приемной антенны средства разведки; $T_{ш_p}$ - шумовая температура разведприемника; L_p - затухание в среде до разведприемника.

Выражения (7) и (8) позволяют определить минимальное отношение сигнал-шум:

$$\left(2\frac{P_c}{N_p}\right)=\frac{G_{прд_p}}{G_{прд}}\frac{G_{прм_p}}{G_{прм}}\frac{L_л}{L_p}\frac{T_{ш_{прм}}}{T_{ш_p}}k_з R\frac{2E_б}{N}=K_0\frac{2E_б}{NT_б}, \qquad (9)$$

где $K_0=\frac{G_{прд_p}}{G_{прд}}\frac{G_{прм_p}}{G_{прм}}\frac{L_л}{L_p}\frac{T_{ш_{прм}}}{T_{ш_p}}k_з$.

Отношение сигнал-шум в линейной части разведприемника:

$$q=\left(\frac{2P_c}{N_p}\right)\frac{1}{F}=K_0\frac{1}{FT_б}\frac{2E_б}{N}. \qquad (10)$$

Положим, что разведуемое средство связи использует сигнал с постоянной спектральной плотностью S_c^2 и полосой Δf_c, что позволяет выбрать в разведприемнике оптимальную полосу пропускания полосового фильтра $F=\Delta f_c$. Учитывая, что $S_c^2=\frac{2P_c}{F}$ выражение (10) можно записать в виде:

$$\left(\frac{S_c^2}{N_p}\right)=K_0\frac{1}{FT_б}\frac{2E_б}{N}. \qquad (11)$$

Если в линейной части разведприемника $\left(\frac{S_c^2}{N_p}\right) << 1$, то энергетическое обнаружение невозможно. Из этого условия следует, что при заданных K_0, $E_б$, N_p, чем больше $FT_б = \frac{B}{2}$, где B - база сигнала, тем меньше отношение $\left(\frac{S_c^2}{N_p}\right)$ и тем больше энергетическая скрытность. Если же $\left(\frac{S_c^2}{N_p}\right) \geq 1$, то сигнал может быть обнаружен.

В конечном виде можно записать выражение для отношения сигнал-шум на выходе разведприемника:

$$q = K_0 \sqrt{t_u F}\, \frac{1}{FT_б}\, \frac{2E_б}{N}. \qquad (12)$$

Будем считать, что выбранный порог h обеспечивает максимальное значение вероятности правильного обнаружения $P_{обн}$, при заданном значении вероятности ложной тревоги $P_{лт}$. Из выражений (9) и (12) можно получить условие перехвата сигнала системы связи:

$$\underbrace{\left(\frac{G_{прм}}{T_{ш_{прм}}}\right)}_{1}\underbrace{\left(\frac{G_{прд}}{G_{прм_p}}\right)}_{2}\underbrace{\left(\frac{L_p}{L_л}\right)}_{3}\underbrace{\left(\frac{1}{k_з}\right)}_{4}\underbrace{\left(1\Big/\left(\frac{2E_б}{N}\right)\frac{1}{T_б}\frac{t_u}{F}\right)}_{5} \leq \underbrace{\left(\frac{G_{прм_p}}{T_{ш_p} h}\right)}_{6}, \qquad (13)$$

где 1 – характеристики приемника, 2 – характеристики передающей антенны; 3 – потери в линии связи; 4 – запас по энергетике; 5 – характеристики модуляции; 6 – характеристика опасности перехвата.

Выражение (13) представляет собой условие энергетической скрытности линии связи в зависимости от ее параметров и характеристик разведприемника. При увеличении базы сигнала B энергетическая скрытность возрастает, даже при выполнении условия $\left(\frac{S_c^2}{N_p}\right) \geq 1$, т.к. $q \equiv \sqrt{\frac{1}{B}}$.

Вероятность ложной тревоги будет равна:

$$P_{лт} = \int_h^\infty \varpi_0 \left(q \right) dq = 1 - \Phi\left(\frac{h-n}{\sqrt{2n}}\right), \qquad (14)$$

где $\varpi_0(q)$ - распределение вероятностей соответствующее отсутствию сигнала; $\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{t^2}{2}} dt$ - интеграл вероятностей; n - число «степеней свободы» сигнала, причем $n \approx B$.

Вероятность правильного обнаружения определяется выражением:

$$P_{обн} = \int_{h}^{\infty} \varpi(q)\, dq = 1 - \Phi\left(\frac{h - (n+q)}{2(n+2q)}\right), \qquad (15)$$

где $\varpi(q)$ - распределение вероятностей соответствующее наличию сигнала.

При $n >> q$ нетрудно заметить, что $P_{обн} \approx P_{лт}$. Это еще раз доказывает тот факт, что для сигналов с большой базой при небольших отношениях сигнал-шум обеспечивается высокая скрытность.

Под **помехоустойчивостью** понимается способность систем связи выполнять возложенные на них задачи с заданным качеством при воздействии на них помех. Поскольку помехоустойчивость зависит от ряда случайных факторов и причин, то количественной мерой ее может служить вероятность нарушения функционирования системы связи при воздействии помех $P_н$. Вероятность $P_н$ можно определить как вероятность того, что фактическое значение отношения сигнал-шум на выходе приемника средства связи станет меньше некоторого критического значения $q_{кр}$, при котором функционирование системы связи нарушается, т.е. $P_н = P(q \le q_{кр})$.

Помехоустойчивость системы связи зависит от сочетания большого числа факторов: вида (формы) помехи, интенсивности помехи, формы полезного сигнала, структуры приемника, антенной системы, применяемых способов борьбы с помехами и т.д. [1]. Остановимся на энергетической помехоустойчивости, которая определяется энергетическими характеристиками сигнала и помехи в предположении различия их по форме и согласования приемника с сигналом при флуктуационной помехе.

Оценим сначала помехоустойчивость приемника сложного сигнала, а затем помехоустойчивость средства связи.

Максимальное отношение сигнала к белому шуму на выходе оптимального приемника не зависит от формы сигнала и равно:

$$q = \frac{2E}{N}. \qquad (16)$$

Следовательно, если сигнал выделяется на фоне только внутренних шумов приемника, то помехоустойчивость приемников, согласованных с сигналами любой формы, будет одинаковой. Если же помеха создается внешним источником,

то удобно представить q в виде отношения мощности сигнала и помехи. Если помеха имеет равномерную спектральную плотность N_n в полосе частот сигнала Δf_c, то для сигнала длительностью T можно записать:

$$q = \frac{2E}{N_n} = \frac{2P_c T}{N_n} \cdot \frac{\Delta f_c}{\Delta f_c} = 2\frac{P_c}{P_n}\Delta f_c T . \qquad (17)$$

Выражение (17) будет справедливо и при действии узкополосной помехи. Если же на вход приемника будет действовать смесь широкополосной и узкополосной помех с мощностями $P_{пш}$ и $P_{пу}$, то:

$$q = 2\frac{P_c}{P_{пш} + P_{пу}}\Delta f_c T . \qquad (18)$$

Оценим общую характеристику помехоустойчивости средства связи при активных помехах (рис.2).

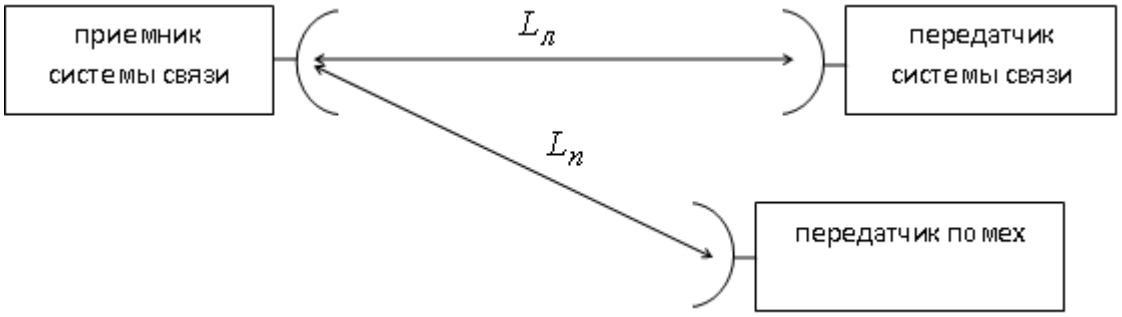

Рис. 2. Схема линии связи и передатчика помех

Условие энергетического подавления радиолинии определим при допущении, что спектральная плотность преднамеренной помехи N_n больше плотности естественного шума N. Тогда критическое отношение сигнал-помеха на выходе приемника радиолинии можно записать:

$$\frac{2P_c}{N_n} = \frac{2RE_б}{N_n} . \qquad (18)$$

Здесь $\frac{2E_б}{N_n}$ - критическое отношение сигнал-помеха, при котором еще обеспечивается заданное качество передачи информации.

Рассмотрим приемник сложного сигнала в полосе частот с равномерным усилением в полосе частот сигнала Δf_c. Учитывая декорреляцию помехи в полосе Δf_c, запишем:

$$N_n = \frac{P_{прд_n} G_{прм_n} G_{прд_n} \delta}{\Delta f_c}, \qquad (19)$$

где $P_{прд}$ - мощность передатчика помех; $G_{прд_n}$ - коэффициент усиления передающей антенны средства активных помех; $G_{прм_n}$ - коэффициент усиления приемной антенны средства связи по боковым лепесткам диаграммы направленности; $\delta = r_k^2 B$; r_k^2 - среднее значение квадрата коэффициента взаимной корреляции сигнала и помехи.

Следовательно, помехоустойчивость в радиолинии будет обеспечена при соблюдении следующего неравенства:

$$\frac{P_{прд} G_{прд} L_n G_{прм}}{P_{прд_n} G_{прд_n} L_л G_{прм_n}} \geq R \frac{2E_б}{N_n}. \qquad (20)$$

Перепишем неравенство в виде аналогичном (13):

$$\underbrace{\left(P_{прд} G_{прд}\right)}_{1} \underbrace{\left(\frac{G_{прм}}{G_{прм_n}}\right)}_{2} \underbrace{\left(\frac{L_n}{L_л}\right)}_{3} \underbrace{\left(\frac{1}{k_з}\right)}_{4} \underbrace{\left(\left[\frac{2\delta R E_б}{\Delta f_c N_n}\right]^{-1}\right)}_{5} \geq \underbrace{\left(P_{прд_n} G_{прд_n}\right)}_{6}, \qquad (21)$$

где 1- характеристика передатчика средства связи; 2 – характеристики антенн приемника; 3 – потери в линии; 4 – коэффициент запаса; 5 – критическое отношение помеха-сигнал; 6 – характеристики передатчика помех.

Выражение $Q = \frac{2\delta R E_б}{\Delta f_c N_n}$ представляет собой параметр, зависящий от вида модуляции сигнала. Так как $\frac{\Delta f_c}{R} = \Delta f_c T_б = \frac{B}{2}$, то $Q = \frac{B}{2\delta E_б / N_n}$.

Анализ выражения (21) позволяет сделать следующие выводы. Во-первых, для характеристик передатчика помех, а также передатчика средства связи удобно использовать произведение мощности передатчика на коэффициент усиления антенны, которое имеет размерность [Вт·дБ]. Эта характеристика позволяет оценивать эффективность различных передатчиков помех. Во-вторых, записанные в левой части выражения (21) сомножители часто являются случайными величинами, особенно при относительном движении передатчика помех и преемника средства связи.

Из сравнения выражений (13) и (21) следует, что одновременное улучшение скрытности и помехоустойчивости достигается увеличением базы сигнала B, а также улучшением направленности антенн передатчика и приемника.

Следовательно, основное направление повышения помехозащищенности средств связи – применение сложных сигналов, фазированных антенных решеток и их комплексирование.

2. Порядок выполнения практического занятия

При подготовке к практическому занятию

На этапе подготовки к практическому занятию студенты должны, используя литературу [1,2] и материалы лекций углубить свои знания по методам повышения помехозащищенности систем связи.

Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.Каждая подгруппа получает от преподавателя индивидуальный вариант задания на практическое занятие, который представляет собой характеристики средств связи и средств радиоэлектронного противодействия.

Студенты должны:

1. Вычислить вероятность правильного обнаружения в зависимости от значений q при различных значениях базы сигнала и вероятности ложной тревоги в соответствии с методикой, изложенной в п.1.2, построить соответствующие графические зависимости.
2. Для заданных исходных данных определить возможность перехвата сигнала разведприемником противника.
3. Для заданных исходных данных определить возможность радиоэлектронного подавления линии радиосвязи противником.

3. Контрольные вопросы

1. Дайте определение помехозащищенности.
2. Что такое помехоустойчивость и скрытность?
3. Перечислите основные меры по повышению помехозащищенности линии связи.
4. От чего зависит возможность радиоэлектронного подавления линии связи?
5. От чего зависит возможность перехвата сигнала средствами радиоразведки противника?
6. Дайте характеристику основным видам скрытности.

Литература

1. Емельянов В.Е., Болелов Э.А. Информационная безопасность телекоммуникационных систем ГА: Учебное пособие. – М.: МГТУ ГА, 2009.

2. Информационная безопасность телекоммуникационных систем (Технические аспекты): Учеб.пособие для вузов / В.Г. Кулаков и др. – М.: Радио и связь, 2004.

Практическое занятие №3
Средства защиты информации, используемые в автоматизированных системах управления воздушным движением и телекоммуникационных системах гражданской авиации

Цель практического занятия – практическое изучение средств защиты информации современных АС УВД «Альфа», «Синтез» и телекоммуникационных систем гражданской авиации.

Время - 4 часа.

1. Основные теоретические сведения

Средства защиты информации, используемые в автоматизированной системе управления воздушным движением (АС УВД) можно разделить на следующие основные типы[1]:

- средства разграничения доступа пользователей к ресурсам АС УВД;
- средства межсетевого экранирования;
- средства анализа защищенности АС УВД;
- средства обнаружения вторжений;
- средства антивирусной защиты.

Вся информация, циркулирующая в АС УВД, не содержит государственной тайны, персональных данных сотрудников или клиентов, но может содержать сведения ограниченного распространения (конфиденциальная информация). ВАСУВД обрабатывается следующая информация: радиолокационная; радиопеленгационная; метеорологическая; плановая.

Краткое описание функциональных возможностей перечисленных выше средств защиты изложено ниже.

Средства разграничения доступа предназначены для защиты от несанкционированного доступа (НСД) к информационным ресурсам АС УВД. Разграничение доступа реализуется средствами защиты на основе процедур *идентификации*, *аутентификации* и *авторизации* пользователей, претендующих на получение доступа к информационным ресурсам АС УВД. На этапе собственной идентификации пользователь предоставляет свой идентификатор, в качестве которого, как правило, используется регистрационное имя учетной записи пользователя. После представления идентификатора проводится проверка истинной принадлежности этого идентификатора пользователю, претендующему на получение доступа к информации АС УВД. Для этого выполняется процедура

аутентификации, в процессе которой пользователь должен предоставить аутентификационный параметр, при помощи которого подтверждается эта принадлежность. Необходимо отметить, что процедура идентификации и аутентификации пользователей в большинстве случаев проводится одновременно, т.е. пользователь сразу предъявляет идентификационные и аутентификационные параметры доступа. В случае успешного завершения процедур идентификации и аутентификации проводится авторизация пользователя, в процессе которой определяется множество информационных ресурсов, с которыми может работать пользователь, а также множество операций, которые могут быть выполнены с этими информационными ресурсами АС УВД. Присвоение пользователям идентификационных и аутентификационных параметров, а также определение их прав доступа осуществляется на этапе регистрации пользователей в АС УВД (см. рис. 1).

Рис. 1. Процедура входа пользователя вАС УВД

Средства разграничения доступа согласно классификационной схеме [1] отнесены к активным средствам защиты, поскольку позволяют блокировать доступ пользователя к информации АС УВД в случае не прохождения им процедур идентификации, аутентификации или авторизации.

Межсетевые экраны (МЭ) реализуют методы контроля за информацией, циркулирующей вАС УВД, поступающей в АС УВД и выходящей из АС УВД, и обеспечения защиты АС УВД посредством фильтрации информации на основе критериев, заданных администратором. Процедура фильтрации включает анализ заголовков каждого пакета, проходящего через МЭ, и передачу его дальше по маршруту следования только в случае, если он удовлетворяет заданным правилам фильтрации. При помощи фильтрования МЭ позволяют обеспечить защиту от сетевых атак путем удаления из информационного потока тех пакетов данных, которые представляют потенциальную опасность дляАС УВД. Фильтрация пакетов данных может осуществляться по параметрам протоколов, относящихся к различным уровням модели взаимодействия открытых систем. Правила

фильтрования пакетов данных, проходящих через МЭ, могут определяться на основе двух базовых методов[1]:

«*все, что не запрещено - разрешено*». Правила фильтрации, построенные на основе этого метода, по существу определяют те типы пакетов, которые должны быть заблокированы МЭ. При этом все остальные пакеты данных, проходящие через МЭ, считаются разрешенными;

«*все, что не разрешено - запрещено*». Правила фильтрации, сформированные на основе данного метода определяют только разрешенные пакеты данных, которые могут поступать или отправляться изАС УВД. При этом МЭ блокирует все остальные проходящие через него пакеты данных. Данный метод позволяет сформировать более строгие правила фильтрации за счет минимизации разрешенных типов пакетов.

МЭ также позволяет скрыть реальные IP-адреса защищаемой АС УВД при помощи функции трансляции сетевых адресов NAT (NetworkAddressTranslation), которая выполняется следующим образом. При поступлении пакета данных в МЭ он заменяет реальный IP-адрес отправителя пакета данных на виртуальный и пересылает измененный пакет получателю (см. рис. 2). При получении ответных пакетов МЭ выполняет обратные действия по замене IP-адресов.

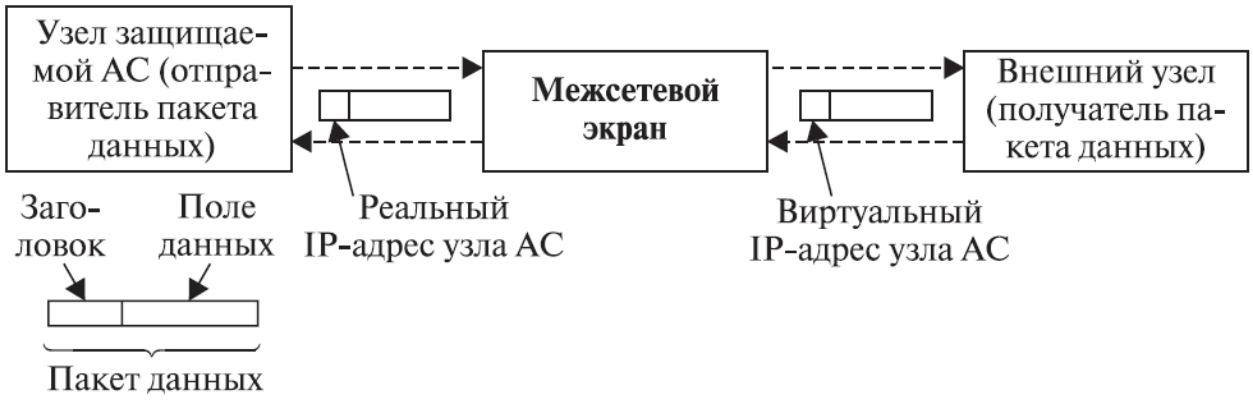

Рис. 2. Схема трансляции IP-адресов в межсетевом экране

Трансляция IP-адресов может осуществляться МЭ в одном из четырех режимов: динамическом, статическом, статическом с динамической выборкой IP-адресов и комбинированном.

Средства анализа защищенности (САЗ) выделены в обособленную группу, поскольку предназначены для выявления уязвимостей в программно-аппаратном обеспечении АС УВД. САЗ являются превентивным средством защиты, которое позволяет выявлять уязвимости при помощи анализа исходных текстов программного обеспечения (ПО) АС УВД, анализа исполняемого кода ПО АС УВД или анализа настроек программно-аппаратного обеспечения АС УВД.

Обнаружение уязвимостей АС УВД путем анализа исходных текстов ПО, как правило, осуществляется посредством составления алгоритма работы программы и последующей проверки отсутствия в нем ошибок, которые могут привести к нарушению информационной безопасности. Алгоритм работы ПОАС УВД может быть составлен в виде блок-схем или формализован при помощи различных математических аппаратов.

Еще одним способом выявления уязвимостей в исходных текстах ПО является поиск типовых конструкций определенного языка программирования, использование которых, как правило, приводит к появлению уязвимостей в программе. Обнаружение уязвимостей ПО АС при помощи анализа исполняемого кода ПО может осуществляться двумя способами.

Первый предполагает запуск программы АС в рамках тестовой среды, в которой проверяется безопасность программы. В процессе выполнения программы для нее формируется ряд тестовых запросов, после чего анализируется реакция программы, т.е. проверяется, каким образом исполняемый код программы влияет на состояние тестовой среды. Если в результате выполнения сформированного запроса тестовая среда переходит в небезопасное состояние, приводящее, например, к нарушению работоспособности АС УВД, то делается вывод о наличие ряда уязвимостей в тестируемой программе. Такой метод обнаружения уязвимостей позволяет выявить ряд ошибок, внесенных на этапе разработки ПО, например, ошибки, приводящие к переполнению буфера, ошибки неправильного доступа к памяти, выход за границы массива данных и др. Основным недостатком рассмотренного метода является отсутствие гарантий обнаружения всех технологических уязвимостей ПО АС УВД, поскольку смоделировать все возможные состояния среды, в рамках которой выполняется программа АС УВД, не представляется возможным.

Второй способ анализа защищенности исполняемого кода ПО предполагает имитацию информационных атак на АС с последующим анализом результатов. По результатам имитирования информационных атак формируется перечень уязвимостей ПОАС УВД. К преимуществам этого метода обнаружения уязвимостей можно отнести простоту реализации, а к недостаткам - невозможность обнаружения уязвимостей АС УВД, описание которых отсутствует в базе данных САЗ.

Для выявления уязвимостей АС УВД можно проводить анализ параметров настроек программно-аппаратного обеспечения системы. В этих целях осуществляется сбор информации о настройках АС УВД, после чего собранные значения сравниваются с эталонными значениями параметров и в случае выявления несоответствий САЗ фиксирует факт наличия уязвимости АС. Данный метод также прост в реализации, однако не позволяет обнаружить уязвимости, описания которых отсутствуют в базе данных метода.

Средства антивирусной защиты предназначены для обнаружения и удаления вредоносного ПО, присутствующего в АС УВД. К таким вредоносным программам относятся компьютерные вирусы, а также ПО типа «троянский конь», «spyware» и «adware».

В настоящее время существует три основных типа антивирусных программ: сканеры, мониторы и гибридные антивирусные средства. Алгоритм работы антивирусного сканера предполагает обнаружение вирусов на основе сигнатур, хранящихся в базе данных сканера. Сигнатура вируса представляет собой последовательность байт, характерную для определенного вируса. Если в процессе анализа файловых ресурсов узлов АС УВД сканер обнаружит фрагмент, соответствующий сигнатуре, хранящейся в его базе данных, то он сигнализирует о выявлении вируса. Недостатком антивирусных сканеров является невозможность обнаружения тех вирусов, сигнатуры которых отсутствуют в базе данных. Для устранения этого недостатка в сканерах используется дополнительный компонент - эвристический анализатор, предназначенный для обнаружения вирусов, заранее неизвестных сканеру. Антивирусный сканер выполняет проверку ресурса на наличие вируса только по команде администратора.

Антивирусные мониторы - это специальные программы, которые функционируют в фоновом режиме операционных систем защищаемых узлов АС УВД и осуществляют проверку всех файловых ресурсов узла. Для обнаружения вирусов антивирусные мониторы используют рассмотренных выше алгоритмы работы антивирусных сканеров.

Средства антивирусной защиты относятся к активным средствам защиты, которые позволяют не только выявить, но и в большинстве случаев удалить из системы вредоносные программы.

Система обнаружения вторжений(СОВ) - это специализированные программные или программно-аппаратные комплексы, предназначенные для выявления информационных атак на ресурсы АС УВД посредством сбора и анализа данных о событиях, регистрируемых в системе. Обобщенная структура СОВ представлена на рис. 3 и включает следующие компоненты:

- модули-датчики, предназначенные для сбора необходимой информации о функционировании АС УВД;
- модуль выявления атак, выполняющий анализ данных, собранных датчиками, с целью обнаружения информационных атак;
- модуль реагирования на обнаруженные атаки;
- модуль хранения данных, в котором содержится вся конфигурационная информация, а также результаты работы средств обнаружения атак;
- модуль управления компонентами средств обнаружения атак.

Рис. 3. Обобщенная структура СОВ

СОВ могут включать два типа датчиков - сетевые и хостовые.

Сетевые датчики предназначены для сбора информации обо всех пакетах данных, передаваемых в рамках того сетевого сегмента, где установлен датчик. Сетевые датчики реализуются в виде отдельного программно-аппаратного блока, подключаемого к сегменту АС УВД.

Хостовые же датчики устанавливаются на рабочие станции или серверы АС УВД и собирают информацию обо всех событиях, происходящих на этих узлах системы.

Как правило, большая часть существующих СОВ используют оба типа датчиков для того, чтобы имелась возможность сбора максимального объема данных, необходимого для обнаружения информационных атак. Результаты работы СОВ записываются в хранилище системы, в качестве которого может выступать обыкновенный текстовый файл или база данных. Управление компонентами СОВ может выполняться удаленным или локальным способом в зависимости от использования той или иной системы. Локальное управление осуществляется непосредственно с того узла, на котором установлен компонент СОВ, а удаленное - посредством команд, посылаемых по каналам связи.

В табл.1 представлены средства защиты информации, используемые в современных АС УВД «Альфа» и «Синтез».

Таблица 1. Средства защиты информации современных АС УВД

Функции защиты информации	**Программно-аппаратные средства защиты информации**
Защита информации от НСД на рабочих станциях и серверах	Комплекс программных средств защиты информации «Барьер-УВД2». Система защиты информации «Сфера»
Антивирусная защита информации	Антивирус Касперского
Анализ защищенности	SecPointPenetratorв мобильном исполнении
Обнаружение вторжений	Комплекс StoneGate IPS
Межсетевое экранирование	StoneGateFirewall

2. Порядок выполнения практического занятия

При подготовке к занятию

На этапе подготовки к практическому занятию студенты должны, используя литературу [1,2] и материалы лекций углубить свои знания системам, средствам и методам защиты информации.

Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем студенты получают от преподавателя необходимую литературу [2-5] и самостоятельно, под руководством преподавателя, изучают средств защиты информации современных АС УВД «Альфа», «Синтез» и телекоммуникационных систем гражданской авиации, обращая внимание на методы, используемые для защиты информации и характеристики средств защиты информации.

3. Контрольные вопросы

1. Что представляет собой комплекс программных средств защиты информации «Барьер-УВД2»?

2. Какие программно-аппаратные средства защиты информации, которые используются в комплексе средств защиты информации АС УВД «Синтез»?

3.Назовите основные характеристики средства защиты информации, которые используются в комплексе средств защиты информации АС УВД «Синтез».

4. Что представляет собой комплекс средств защиты информации «Сфера»?

5. Какие подсистемы входят в комплекс средств защиты информации «Сфера»?

6.Назовите основные методы, используемые для защиты информации вАС УВД «Альфа».

7. Как осуществляется настройка подсистем защиты информации комплекса «Сфера»?

8. Назовите состав персонала, обслуживающего комплекс средств защиты информации АС УВД «Альфа» и «Синтез» и их должностные обязанности.

Литература

1. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учеб.пособие/В.А. Сердюк; Гос.ун-т – Высшая школа экономики.- М: Изд. Гос.ун-та – Высшей школы экономики, 2011.

2. Техническое описание. Комплекс средств защиты информации. Часть 2. Книга 6. Том 1.

3. Комплекс программных средств «Система защиты информации «Сфера». Описание программы. НКПГ.10301 13-01. ООО «Фирма «Нита», 2005.

4. Комплекс программных средств «Система защиты информации «Сфера». Руководство оператора. НКПГ.10301 02 34 01. ООО «Фирма «Нита», 2005.

5. Комплекс программных средств «Система защиты информации «Сфера». Руководство системного программиста. НКПГ.10301 02 32 01. ООО «Фирма «Нита», 2005.

Практическое занятие №4
Методика определения актуальности угроз информационной безопасности вАС УВД

Цель практического занятия – практическое изучение методики определения актуальности угроз информационной безопасности в АС УВД.

Время - 6 часов.

1. Основные теоретические сведения

При оценке актуальности угроз информационной безопасности вАС УВД используются следующие исходные данные[1,3]:

1) перечень источников угроз;

2) перечень угроз безопасности;

3) значения коэффициентов опасности выполнения деструктивных действий;

4) значения вероятностей наличия благоприятных условий для использования уязвимостей в интересах реализации угроз безопасности информации.

В качестве показателя актуальности угрозы безопасности информации, при наличии источника угрозы принимается двухкомпонентный вектор, первой компонентой которого является *коэффициент опасности угрозы*, а второй – *вероятность реализации угрозы*.

Коэффициент опасности угрозы $\overline{D}_j$ вычисляется по коэффициенту опасности деструктивных действий и матрице взаимосвязи угрозы и деструктивными действиями, возможными при реализации угрозы, по формуле:

$$\overline{D}_j = \begin{cases} \sum_{r=1}^{R}\sum_{g=1}^{G} \tau_{jg}\varepsilon_{gr}p'_{jr}, \sum_{r=1}^{R}\sum_{g=1}^{G} \tau_{jg}\varepsilon_{gr}p'_{jr} < 1; \\ 1, \sum_{r=1}^{R}\sum_{g=1}^{G} \tau_{jg}\varepsilon_{gr}p'_{jr} \geq 1, \end{cases} . \qquad (1)$$

где: τ_{jg} - элемент матрицы $\mathbf{T} = \|\tau_{jg}\|, j = \overline{1,J}, g = \overline{1,G}$, определяемый следующим образом: если j-я угроза приводит к реализации g-го деструктивного действия, то $\tau_{jg} = 1$, в противном случае - $\tau_{jg} = 0$;

ε_{gr} - элемент матрицы $\mathbf{E} = \|\varepsilon_{gr}\|, r = \overline{1,R}, g = \overline{1,G}$, который представляет собой коэффициент опасности g-го деструктивного действия, выполняемого в результате реализации угрозы относительно r-го блока информации;

p'_{jr} - вероятность реализации j-й угрозы в отношении к r-му блоку информации.

Вероятность реализации угрозы характеризует динамику возникновения и реализации угрозы. В рамках данного анализа принято, что для угроз связанных с несанкционированным доступом, вероятность реализации угрозы в условиях отсутствия мер защиты приравнивается к единице, если данная угроза имеет место, и к нулю, если угроза отсутствует.

Таким образом, относительно каждого блока информации определяется только вероятность наличия благоприятных условий для реализации угрозы, а затем в зависимости от содержания угрозы рассчитывается по формулам вероятность j-й угрозы как функции только от вероятности в отношении хотя бы одного блока информации или в отношении одновременно нескольких блоков.

Вероятность реализации j-й угрозы (в общем случае как функция времени) в отношении хотя бы одного блока информации определяется по формуле:

$$P_j = 1 - \prod_{r=1}^{R} (1 - p_j^* p'_{jr}), \quad (2)$$

а в отношении одновременно R блоков информации по формуле:

$$P_j = 1 - \prod_{r=1}^{R} (1 - p_j^* p'_{jr}), \quad (3)$$

где p_j^* - вероятность наличия благоприятных условия для реализации j-й угрозы:

$$p_j^* = 1 - \prod_{k=1}^{K} (1 - p''_{jk}), \quad (4)$$

где p''_{jk} - вероятность того, что могут сложиться благоприятные условия для использования k-й уязвимости в интересах j-й угрозы.

Угроза признается актуальной, если показатель ее актуальности, представленный в вербальной интерпретации, попадает в заштрихованную область (см. табл. 1).

Таблица 1. Вербальная интерпретация показателей актуальности угрозы безопасности информации.

		Вероятность реализации угрозы				
		Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Коэффициент опасности угрозы	Очень низкий					
	Низкий					
	Средний					
	Высокий					
	Очень высокий					

Пример вербальной интерпретация вероятности реализации и коэффициента опасности угрозы представлен в табл.2.

Таблица 2. Пример вербальной интерпретация вероятности реализации и коэффициента опасности угрозы

Минимальное значение показателя	Максимальное значение показателя	Вербальная интерпретация
0	0,2	Очень низкое
0,2	0,4	Низкое
0,4	0,6	Среднее
0,6	0,85	Высокое
0,85	1	Очень высокое

Под **источником угрозы безопасности информации** понимается субъект, который может реализовать угрозу безопасности информации. Источники угроз определяются экспертным способом. Экспертам задаются вопросы, ответам присваивается соответствующий индекс. Пример анкеты, определяющей возможные источники угроз, представлен в табл.3.

Таблица 3. Анкета определения возможных источников угроз

Содержание вопроса	Возможные варианты ответов	Индекс ответа
Имеются ли у организации, которое эксплуатирует АС УВД конкуренты?	Да	Ио1
	Нет	Ио2
Будет ли обрабатываться вАС УВД информация, которая может заинтересовать иностранные спецслужбы?	Да	Ио3
	Нет	Ио4
Имеется ли вАС УВД информация, которая может заинтересовать криминальные элементы и террористические организации?	Да	Ио5
	Нет	Ио6
Могут ли сотрудники устанавливать самостоятельно, по собственному усмотрению новое программное обеспечение?	Да	Ио7
	Нет	Ио8
Имеет ли АС УВД выход в Internet или другие глобальные сети?	Да	Ио9
	Нет	Ио10
Имеет ли в организации, эксплуатирующей АС УВД внешняя АТС	Да	Ио11
	Нет	Ио12
Имеется ли в АС УВД не сертифицированное программное обеспечение, разработанное внешними организациями или посторонними лицами?	Да	Ио13
	Нет	Ио14

Состав источников угроз безопасности, в соответствии с индексами ответов, определяется по табл.4.

Таблица 4. Определение состава источников угроз безопасности информации

Индекс ответа	Источник угрозы					
	Конкуренты	Зарубежные спецслужбы	Криминальные и террористические организации	Персонал АС УВД	Хакеры	Разработчики программно-аппаратного обеспечения АС УВД
	ИУ1	ИУ2	ИУ3	ИУ4	ИУ5	ИУ6
Ио1	+					
Ио2						
Ио3						
Ио4		+				
Ио5			+			
Ио6						
Ио7						
Ио8				+		
Ио9						
Ио10					+	
Ио11						
Ио12					+	
Ио13						
Ио14						+

Полный перечень угроз информационной безопасности представлен в [1-3]. Основные типы угроз:

- угрозы физического доступа;
- угрозы непосредственного доступа в операционную систему компьютера или сети с применением программных или программно-аппаратных средств;
- угрозы удаленного доступа в операционную систему компьютера или сеть с применением программных или программно-аппаратных средств;
- непреднамеренные антропогенные угрозы.

Опасность выполнения деструктивного действия определяется его содержанием и важностью информации, на которую направлено это действие. Опасность каждого g-го деструктивного действия для информации, содержащейся в r-м блоке информации, описывается в виде тройки коэффициентов $V_{gr\alpha}$, $V_{gr\beta}$, $V_{gr\gamma}$, где α, β, γ- индексы, отражающие

составляющие опасности, связанные с нарушением конфиденциальности, целостности и доступности соответственно. В общем случае эти коэффициенты могут быть функциями времени.

Коэффициент опасности каждого g-го деструктивного действия в отношении ***r***-го блока информации без учета мер защиты определяется из соотношения:

$$\varepsilon_{gr} = \begin{cases} \delta_{g\alpha}V_{gr\alpha} + \delta_{g\beta}V_{gr\beta} + \delta_{g\gamma}V_{gr\gamma}, \delta_{g\alpha}V_{gr\alpha} + \delta_{g\beta}V_{gr\beta} + \delta_{g\gamma}V_{gr\gamma} \le 1, \\ 1, \delta_{g\alpha}V_{gr\alpha} + \delta_{g\beta}V_{gr\beta} + \delta_{g\gamma}V_{gr\gamma} > 1, \end{cases} \quad (5)$$

где $\delta_{g\alpha}$, $\delta_{g\beta}$, $\delta_{g\gamma}$ - функции, значение которых равно 1, если в результате реализации g-го деструктивного действия нарушается конфиденциальность, целостность и доступность информации, соответственно.

Под **важностью информации** понимается качественная характеристика, определяющая ценность информации для обеспечения функционирования АС УВД, а, следовательно, нежелательность или недопустимость ее несанкционированного уничтожения, модификации, блокировки, распространение вне установленной сферы применения. Важность информации рассматривается как важность обеспечения ее конфиденциальности, целостности и доступности. Для оценки важности этой информации каждому информационному ресурсу присваивается три метки, характеризующие степень важности этой информации с позиции обеспечения ее конфиденциальности, целостности и доступности.

При определении степени важности приняты следующие правила:

- если в блоке информации (файле текстовом, графическом, файле базы данных и т.д.) имеется защищаемая информация, то весь блок подлежит защите и ему присваивается соответствующая степень важности;
- градация важности информации с позиции обеспечения ее конфиденциальности определяется с учетом ее влияния на функционирование АС УВД;
- градация важности информации с позиции обеспечения ее целостности или доступности определяется с учетом уровня ущерба, который может быть в результате нарушения функциональности АС УВД, а также приемлемости затрат (времени, трудовых ресурсов, финансовых затрат) на восстановление целостности или доступности самой информации;
- исполняемые файлы прикладных программ, запуск которых обуславливает доступ к файлам с данными пользователя, имеют не меньшую важность с позиции обеспечения их целостности и (или) доступности, чем сами файлы с данными пользователя;
- если в помещении хранится информация оАС УВД конфиденциального характера или помещение предназначено для конфиденциальных переговоров, то

считается, что возможна утечка информации с наибольшей степенью важности для данного помещения.

Градация важности информации представлена в табл.5.

Таблица 5. Градация важности информации

В интересах обеспечения конфиденциальности	1 степень	для информации, нарушение конфиденциальности которой может привести к ее использованию для вывода АС УВД из строя
	2 степень	для информации, нарушение конфиденциальности которой может привести к ее использованию для вывода из строя отдельных подсистем АС УВД
	3 степень	для информации, нарушение конфиденциальности которой может привести к ее использованию в интересах ухудшения характеристик функционирования АС УВД в целом
	4 степень	для информации, нарушение конфиденциальности которой может привести к ее использованию в интересах ухудшения характеристик функционирования отдельных подсистем АС УВД
	5 степень	для информации, нарушение конфиденциальности которой не является существенным для функционирования АС УВД
В интересах обеспечения целостности	1 степень	для информации, нарушение целостности которой недопустимо, так как исключает возможность функционирования АС УВД
	2 степень	для информации, нарушение целостности которой нежелательно, так как приводит к временной задержке выполнения функций АС УВД
	3 степень	для информации, нарушение целостности которой не является существенным для пользователя
В интересах обеспечения доступности	1 степень	для информации, нарушение доступности которой недопустимо, так как приводит к нарушению функциональности АС УВД, независимо от того восстанавливается доступность или нет
	2 степень	для информации, нарушение доступности которой нежелательно, так как приводит к задержке выполнения функций АС УВД
	3 степень	для информации, нарушение доступности которой не является существенным для пользователя

Перечень деструктивных действий, выполняемых в результате реализации угроз представлен в табл. 6.

Таблица 6. Перечень деструктивных действий

g	Описание деструктивного действия
1	Копирование (чтение) информации
2	Перехват информации
3	Уничтожение информации (носители информации)
4	Модификация, запись новой информации (в том числе инсталляция программного продукта, запись вируса, изменение служебной информации, изменение правил разграничения доступа)
5	Блокирование (в том числе сбои в электропитании, вывод из строя элементов компьютерной техники без уничтожения носителя информации, исключающий возможность работы на ней и требующий ремонтно-восстановительных работ) информации
6	Разглашение информации
7	Хищение информации (в том числе утеря носителя информации, передача отчуждаемого носителя с записанной на нем информацией постороннему лицу)

Зависимость коэффициента опасности деструктивных действий от категории и степени важности информации представлена в табл. 7.

Таблица 7. Зависимость коэффициента опасности деструктивных действий от категории важности информации

Деструктивные действия	Категория важности										
	α					β			γ		
g	1	2	3	4	5	1	2	3	1	2	3
1	1	0,9	0,8	0,4	0,1						
2						1	0,7	0,3	1	0,7	0,3
3						1	0,7	0,3	1	0,7	0,3
4									1	0,7	0,3
5	1	0,9	0,7	0,4	0,2	1	0,6	0,2	1	0,6	0,2
6	1	0,9	0,7	0,4	0,2	1	0,6	0,2	1	0,6	0,2
7	1	0,9	0,7	0,4	0,2	1	0,6	0,2	1	0,6	0,2

Определение вероятностей наличия благоприятных условий для создания уязвимостей основано на опросных данных. Пример анкеты опросов для одной уязвимости ($k=18$) представлен в табл.8. В случае, когда для наличия благоприятных условий существует несколько причин, вероятность вычисляется по следующей формуле:

$$p''_k\left(\sum_{m=1}^{M} a_m\right) = p''_k\left(\sum_{m=1}^{M-1} a_m\right) + p''_k\ a_m\ - p''_k\left(\sum_{m=1}^{M-1} a_m\right) p''_k\ a_m\ , \quad (6)$$

где a_m - m-я причина возникновения благоприятных условий для использования уязвимостей, которая определяется следующим образом: если m-я причина создает k-ю уязвимость, то a_m=1, в противном случае - a_m=0.

Таблица 8. Анкета определения вероятностей наличия благоприятных условий для создания уязвимостей

Индекс уязвимос-ти	k	Описание уязвимости звена	m	Вопрос	Ответ	p'_{km}	p''_k
УЗ 2.3	18	Сетевые протоколы и службы	1	Имеется ли подключение к сетям общего пользования	Да	1	
					Вполне вероятно	0,9	
					Возможно	0,8	
					Маловероятно	0,4	
					Нет	0	
			2	Имеют ли доступ в операционную среду АРМ подключенных к АС УВД или сетевому оборудованию обслуживающий персонал (уборщицы, техники и т.д)	Да	1	
					Вполне вероятно	0,8	
					Возможно	0,6	
					Маловероятно	0,3	
					Нет	0	
			3	Имеются ли в штате организации сотрудники, заинтересованные в неправомерном использовании информации АРМ, входящих в состав АС, и обладающие квалификацией в области сетевых технологий	Да	1	
					Вполне вероятно	0,9	
					Возможно	0,8	
					Маловероятно	0,4	
					Нет	0	

В соответствие с выражением:

$$p_j^* = 1 - \prod_{k=1}^{K} 1 - p''_{jk}\ , \quad (7)$$

определяется вероятность наличия благоприятных условий для реализации j-й угрозы.

2. Порядок выполнения практического занятия

При подготовке к занятию

На этапе подготовки к практическому занятию студенты должны, используя литературу [1-3] и материалы лекций углубить свои знания по методике оценки актуальности угроз информационной безопасности.

Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к практическому занятию. Затем преподаватель разбивает группу студентов на подгруппы. Для каждой подгруппы преподаватель определяет подсистему АС УВД (комплекс средств автоматизации (КСА) УВД, комплекс средств планирования использования воздушного пространства (КСА ПИВП), комплекс средств автоматизации аэродромных командно-диспетчерских пунктов (КСА АКДП), комплекс средств автоматизации метеорологического обеспечения (КСА МЕТЕО), комплекс средств обеспечения справочной информацией (КОСИ)) и выдает необходимые для расчетов исходные данные.

Студенты должны:

1. Используя изложенную методику [3] определить показатели актуальности угроз безопасности информации для заданной подсистемы АС УВД.
2. Сформулировать рекомендации по нейтрализации угроз информационной безопасности для заданной подсистемы АС УВД.
3. Определить схему построения защиты для заданной подсистемы АС УВД.

3. Контрольные вопросы

1. Сформулируйте общие положения методики расчета актуальности угроз информационной безопасности АС УВД.
2. Что является исходными данными при оценке актуальности угроз информационной безопасности в АС УВД?
3. Как определятся важность информации, циркулирующей в АС УВД?

Литература

1. Техническое описание. Комплекс средств защиты информации. Часть 2. Книга 6. Том 1.
2. РД ФСТЭК «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», 2007.
3. РД ФСТЭК «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», 2007.