П. 7 Комплекс моделей процессов несанкционированного доступа к ресурсам системы

П.7.1 Модель без учета периода объективной ценности защищаемых ресурсов

Настоящая модель справедлива для оценки защищенности ресурсов без учета периода их объективной ценности, т.е. лишь исходя из реализуемой технологии защиты. Другими словами, защищаемые ресурсы полагаются априори ценными в течение бесконечного периода времени.

Построение вероятностного пространства для оценки отсутствия воздействий в результате НСД осуществляется в предположении реализации в системе элементов защиты ресурсов от потенциального нарушителя. В приложении к ИС защищаемыми являются в первую очередь информационные и программные ресурсы. Однако, модель является более общей, в качестве защищаемых могут выступать людские, материальные, финансовые и др. ресурсы.

Для доступа к хранимым в системе ресурсам выстраивается последовательность преград от злоумышленника с тем, чтобы допущенный пользователь, зная и реализуя алгоритм преодоления этих преград, мог решать свои задачи в установленном штатном режиме. В качестве нарушителя рассматривается лицо, не посвященное в тайну преодоления защитных преград. Вскрывая каким-либо доступным образом алгоритм преодоления преград, злоумышленник вполне может получить доступ к ресурсам системы.

Рассматривается наиболее тяжелый режим функционирования системы защиты в ожидании постоянной угрозы ее вскрытия. Нарушитель в состоянии проникнуть в систему лишь при условиях, что

- во-первых, ему станет известна система защиты в части, необходимой для достижения его целей;
- во-вторых, он успеет получить доступ к информационным и/или программным ресурсам системы до того, как эта система защиты видоизменится (после чего перед нарушителем возникнет проблема повторного преодоления защитных преград).

При моделировании действия «умного» нарушителя, оснащенного возможными высокотехнологичными средствами вскрытия системы зашиты, могут быть охарактеризованы лишь большей скоростью преодоления защитных преград.

Суть формализации отражена на рис. П.7.1:

Рис. П.7.1 Иллюстрация доступа к защищаемым ресурсам

Справедливо следующее утверждение.

Утверждение П.7.1 [36]. При условии существования стационарных распределений исходных характеристик системы защиты ресурсов вероятность предотвращения НСД:

$$P_{защ} = 1 - \prod_{m=1}^{M} P_{НСД\,m}, \qquad (П.7.1)$$

где M – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам;

$P_{НСД\,m}$ — вероятность преодоления нарушителем m-й преграды:

$$P_{НСД\,m} = \frac{1}{f_m} \int_0^{\infty} [1 - F_m(t)]\, U_m(t)\, dt; \qquad (П.7.2)$$

$F_m(t)$ — ФР времени между соседними изменениями защитных параметров m-й преграды (приводящих к необходимости новой их расшифровки нарушителем), f_m – среднее;

$U_m(t)$ — ФР времени расшифровки (вскрытия) значений параметров m-й преграды, u_m – среднее (для средств защиты с неизменяемыми параметрами в качестве среднего может выступать время наработки СЗИ на ошибку или отказ $T_{нар.m}$).

Доказательство. Для получения доступа к ресурсам нарушителю необходимо преодолеть и 1-ю, и 2-ю … и последнюю преграду, вероятность чего равна $\prod_{m=1}^{M} P_{НСД_m}$. Дополнение этой вероятности до 1 есть ничто иное, как искомая вероятность предотвращения НСД, т.е. выражение (П.7.1) доказано. Для доказательства (П.7.2) рассмотрим случайный процесс $\xi_{НСД}(t)$, характеризующий состояние одной преграды с точки зрения защищенности от НСД. Величина $\xi_{НСД}(t)$ в приложении к конкретной m-й преграде может принимать одно из двух значений:

$$\xi_{НСД}(t) = \begin{cases} \textit{«Имеет место несанкционированное преодоление преграды»,} \text{ если к моменту t нарушитель преодолел данную преграду;} \\ \textit{«Отсутствуют несанкционированные преодоления преграды»} \text{ в остальных случаях} \end{cases}$$

Построим случайный процесс $\xi(t)$, $0 \le t < \infty$ следующим образом:

$$\xi(t) = \begin{cases} \xi_1(t) \text{ при } 0 \le t_1 < z_1, \\ \xi_2(t) \text{ при } z_1 \le t < z_1 + z_2, \\ \ldots \\ \xi_k(t) \text{ при } t_{k-1} \le t < t_k, \end{cases}$$

где $t_0=0$, $t_k=z_1+z_2+\ldots+z_k$, $k \ge 1$;

z_k – случайная величина, определяющая интервал времени между $(k-1)$-м и k-м последовательными сменами хотя бы одного из параметров m-й преграды системы и имеющая ФР $F_m(t)$;

$\xi_k(t)$ – случайная функция, определенная на k-ом интервале и принимающая на нем те же значения, что и $\xi_{НСД}(t)$.

Определенный таким образом процесс $\xi(t)$ является регенерирующим, моменты t_k – моментами регенерации, а пара (z_k, ξ_k), $k \geq 1$ – циклами регенерации.

Рассмотрим функцию $\mu(t)=P\{\xi(t)=$«*Имеет место несанкционированное преодоление преграды*»$, z_k>t\}$, определяющую вероятность того, что на k-ом цикле нарушитель преодолел преграду к моменту t, а следующая смена параметров преграды произошла после t. Поскольку ФР $F_m(t)$, $U_m(t)$ независимы, имеем:

$\mu(t) = \int_t^{\infty} d\,F_m(t)U_m(t)$. Далее введем функцию $M(t) = \int_0^t \mu(t-x)d\,F_m^{*n}(x)$, где $F_m^{*n}(t)$ – n-я свертка ФР $F_m(t)$.

Функция $M(t)$ непосредственно интегрируема по Риману на $[0,\infty)$ при $n=0$, поскольку $M(t)=\mu(t)$. Это условие является необходимым для применения предельной теоремы для регенерирующих процессов, согласно которой

$$P_{НСД\ m} = \lim_{t\to\infty} P\left\{\begin{array}{l}\xi(t) = "Имеет\quad место\quad несанкционированное \\ \quad преодоление\quad преграды", z_k > t\end{array}\right\} = \frac{1}{f_m}\int_0^{\infty}\mu(t)dt.$$

Отсюда и следует справедливость утверждения. *Доказательство утверждения П.7.1 завершено*.

В инструментариях реализованы варианты:

а) $F_m(t) = \begin{cases} 0, t \le f_m, \\ 1, t > f_m \end{cases}$ – характеризует случай строго периодической смены параметров m-й преграды;

б) $F_m(t) = 1 - exp\left(-t / f_m\right)$ – характеризует случай нестрогого соблюдения периодичности смены параметров m-й преграды;

в) $U_m(t) = 1 - exp(-t/u_m)$ или для средств защиты с неизменяемыми параметрами $U(t) = 1 - exp(-t/T_{нар.m})$.

П.7.2 Модель с учетом периода объективной ценности ресурсов

Модель П.7.1 справедлива для оценки защищенности ресурсов в случае, когда период объективной их ценности стремится к бесконечности. Однако, на практике чаще всего возникают случаи, когда этот период существенно ограничен. Примером могут служить информационные ресурсы, используемые для выполнения конкретной задачи. По выполнении задачи объективная ценность этих ресурсов может исчезать. Другим примером могут служить наличные финансовые или золотовалютные ресурсы в банке после их поступления на хранение. В этом случае с точки зрения системы защиты банка от НСД период объективной ценности ресурсов совпадает с периодом их нахождения в хранилищах банка. Наконец, третий пример касается системы управления воздушным судном, рычаги которой сосредоточены в кабине пилотов. С точки зрения безопасности полета в условиях террористических угроз период объективной ценности этих ресурсов практически совпадает с длительностью полета или, если самолет захвачен – с длительностью его удержания террористами.

Таким образом, период объективной ценности (ПОЦ) ресурса – это такое время, свойственное ресурсу, по истечении которого ресурс утрачивает свою былую ценность и объективно не нуждается в защите от НСД.

Для настоящей модели с учетом ПОЦ ресурсы считаются защищенными от НСД, если в результате НСД проникновение к ним не осуществлено после истечения их ПОЦ.

Суть формализации на примере преодоления одной из преград отражена на рис. П.7.2:

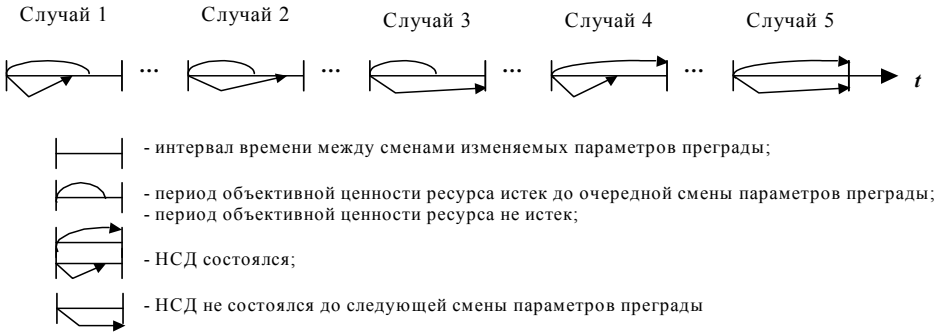

Рис. П.7.2. Формализация процессов НСД с учетом ценности ресурсов

Случай 1 – НСД осуществлен до истечения ПОЦ ресурсов. Случай 2 – НСД осуществлен после истечения ПОЦ ресурсов. Случай 3 – НСД не состоялся. Случай 4 – НСД осуществлен, и период объективной ценности ресурсов дольше, чем время между соседними сменами параметров системы защиты. Случай 5 – параметры системы защиты сменились раньше, чем истек ПОЦ ресурсов и осуществлен НСД (для нарушителя требуется повторное преодоление преграды).

Здесь ресурсы оказались защищенными от НСД в случаях 2, 3, 5 и незащищенными в случаях 1, 4.

Утверждение П.7.2 [36]. При условии существования стационарных распределений учитываемых характеристик, их независимости и при экспоненциальном распределении ПОЦ защищаемых ресурсов стационарная вероятность $P_{НСД\ ПОЦ\ m}$ преодоления отдельной преграды в период сохранения объективной ценности ресурсов существует и равна

$$P_{НСД\ \ ПОЦ_m} = \frac{1}{f_m}\int_0^{\infty} dt \int_t^{\infty} d\,F_m(\tau)\int_0^t d\,U_m(\theta)\left[1 - H(\theta)\right], \qquad (П.7.3)$$

где $F_m(t)$ – ФР времени между соседними изменениями защитных параметров m-й преграды, $m \geq 1$, f_m – среднее;

$U_m(t)$ – ФР времени расшифровки (вскрытия) значений параметров m-й преграды, u_m (или $T_{нар.m}$) – среднее (аналогично модели П.7.1);

$H(t)$ – ФР периода объективной ценности защищаемых ресурсов системы, h – среднее.

Доказательство. Рассмотрим случайный процесс $\xi_{ПОЦ}(t)$, характеризующий состояние преграды с точки зрения защищенности от НСД в период сохранения объективной ценности ресурсов.

$$\xi_{\text{ПОЦ}}(\text{t}) = \begin{cases} \textit{«Имеет место несанкционированный доступ к ресурсам до завершения ПОЦ»,} \text{ если к моменту } t \text{ нарушитель преодолел преграду, а ПОЦ не истек;} \\ \textit{«Отсутствует несанкционированный доступ к ресурсам до завершения ПОЦ»} \text{ в остальных случаях} \end{cases}$$

Построим случайный процесс $\xi(t)$, $0 \le t < \infty$ следующим образом:

$$\xi(t) = \begin{cases} \xi_1(t) \text{ при } 0 \le t_1 < z_1, \\ \xi_2(t) \text{ при } z_1 \le t < z_1 + z_2, \\ \ldots \\ \xi_k(t) \text{ при } t_{k-1} \le t < t_k, \end{cases}$$

где $t_0=0$, $t_k=z_1+z_2+\ldots+z_k$, $k \ge 1$;

z_k – случайная величина, определяющая интервал времени между (k-1) и k-м последовательными сменами хотя бы одного из параметров защитной преграды и имеющая ФР $F(t)$;

$\xi_k(t)$ – случайная функция, определенная на k-ом интервале и принимающая на нем те же значения, что и $\xi_{ПОЦ}(t)$.

Определенный таким образом процесс $\xi(t)$ является регенерирующим, моменты t_k – моментами регенерации, а пара (z_k, ξ_k), $k \ge 1$ – циклами регенерации.

Требование экспоненциальности ФР $H(t)$ используется при формализации ПОЦ. Согласно предположению об экспоненциальности остаток времени до завершения ПОЦ всегда имеет то же распределение $H(t)$ с тем же параметром, это – свойство отсутствия последействия.

Рассмотрим функцию $\mu(t)=P\{\xi(t)=$«Имеет место несанкционированный доступ к ресурсам до завершения ПОЦ»$, z_k>t\}$, определяющую вероятность того, что на k-ом цикле несанкционированное преодоление преграды произошло до истечения ПОЦ к моменту t, а следующая смена параметров преграды произошла после t. Поскольку случайные величины, характеризуемые ФР $F_m(t)$, $U_m(t)$, $H(t)$ независимы, имеем:

$$\mu(t) = \int_t^\infty d\,F_m(\tau) \int_0^t d\,U_m(\theta)[1 - H(\theta)].$$

Далее введем функцию $M(t) = \int_0^t \mu(t-x)\,d\,F_m^{*n}(x),$

где $F^{*n}(x)$, $n \ge 0$ – n-я свертка ФР $F_m(t)$.

Функция $M(t)$ непосредственно интегрирует по Риману на $[0,\infty)$ при $n=0$, поскольку $M(t)=\mu(t)$. Это условие является необходимым для применения предельной теоремы для регенерирующих процессов, согласно которой

$$P_{НСД\ ПОЦ\ m} = \lim_{t\to\infty} P\left\{ \begin{array}{l} \xi(t) = "Имеет\ \ место\ \ несанкционированный \\ \ \ доступ\ \ к\ \ ресурсам\ \ до\ \ завершения\ \ ПОЦ",\ z_k > t \end{array} \right\} = \frac{1}{f_m} \int_0^\infty \mu(t)dt.$$

Отсюда и следует справедливость утверждения. *Доказательство утверждения П.7.2 завершено*.

Аналогично (П.7.1) вероятность защищенности от НСД с учетом ПОЦ равна:

$$P_{защ.ПОЦ} = 1 - \prod_{m=1}^{M} P_{НСД\ \ ПОЦ\ \ m}, \quad \text{(П.7.4)}$$

где M — количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам;

$P_{НСД\ ПОЦ\ m}$ — вероятность преодоления нарушителем m-й преграды до истечения ПОЦ.

В инструментарии КОК реализованы варианты:

а) $F_m(t) = \begin{cases} 0, t \le f_m, \\ 1, t > f_m \end{cases}$ – характеризует случай строго периодической смены параметров m-й преграды (в КОК расчетные значения вероятности сохранения конфиденциальности обозначаются как $P_{конф.строг.}$, графики отображаются оттенками зеленого цвета);

б) $F_m(t) = 1 - exp(-t / f_m)$ – характеризует случай нестрогого соблюдения периодичности смены параметров m-й преграды;

$U(t)=1-exp(-t/u_m)$ или для средств защиты с неизменяемыми параметрами $U(t) = 1 - exp(-t/T_{нар.m})$.

$H(t) = 1- exp(-t/h)$.

Модель П.7.2 реализована в подсистеме «Конфиденциальность» инструментария КОК. В частности, конфиденциальность информации считается сохраненной, если, в результате НСД проникновение к информационным ресурсам не осуществлено или осуществлено после истечения периода объективной конфиденциальности информации (ПОЦ для информационных ресурсов).

Необходимые для моделирования исходные количество преград k и пределы значений u_m определяют в результате дополнительного моделирования, натурных экспериментов, учитывающих специфику системы защиты и возможные сценарии действий нарушителей, или сравнения с аналогами. Их указывают в конструкторской документации в приложении к возможным сценариям НСД, конкретизирующим требования ТЗ в части обеспечения безопасности информации, а значения f_m – в эксплуатационной документации.

Примечание – С учетом специфики расчет $P_{преод\ m}$ для некоторых из преград может быть осуществлен с использованием модели П.6, в этом случае $P_{преод\ m}=1-P_{возд}$, где вероятность отсутствия опасного воздействия в результате НСД $P_{возд}$ вычисляют по формулам модели П.6.

Явные аналитические формулы, реализованные в нструментальных комплексах, получаются на основе интегрирования (по Лебегу) обычными методами выражений (П.7.2) и (П.7.3) и использования выражений (П.7.1) и (П.7.4).