УДК 004.056

ОБОБЩЕННАЯ МОДЕЛЬ ЭЛЕМЕНТАРНОЙ ЗАЩИТЫ ПРОГРАММНОГО СРЕДСТВА

Алекперов И.Д.

к.т.н., доцент

ЧОУ ВО «Южный университет (ИУБиП)»

e–mail: ilgar@iubip.ru

Гуденко В.И.

Аспирант 1 года обучения

ЧОУ ВО «Южный университет (ИУБиП)»

e–mail: v_gudenko@iubip.ru

Инкин П.А.

Аспирант 1 года обучения,

ЧОУ ВО «Южный университет (ИУБиП)»

e–mail: e_inkin@iubip.ru

Аннотация: Создание эшелонированной системы защиты, позволяет обеспечить безопасность информации от нелегитимного доступа разрушающих программных средств и увеличить защитное свойство ее преграды. Ценность предмета защиты не зависит от времени. Прочность защиты зависит от свойств преграды.
Ключевые слова: безопасность информации, нелегитимный доступ, защита информации, уровень безопасности, прочность защиты, предмет защиты, преграда, нелегитимный доступ к предмету защиты, эшелонированная система защиты.

GENERALIZED MODEL OF ELEMENTARY SOFTWARE PROTECTION

I.D. Alekperov

V.I. Gudenko

P.A. Inkin

Abstract: Creating a layered security system allows you to ensure the security of information from illegitimate access to destructive software and increase the protective property of its barrier. The value of the protection item does not depend on time. The strength of the protection depends on the properties of the barrier.
Keywords: information security, illegitimate access, information protection, security level, strength of protection, subject of protection, barrier, illegitimate access to the subject of

protection, layered protection system.

Повышение эффективности обеспечения информации от нелегитимного доступа разрушающих программных средств – программных закладок может быть проведено за счет создания эшелонированной системы защиты, позволяющей увеличить защитное свойство ее преграды.

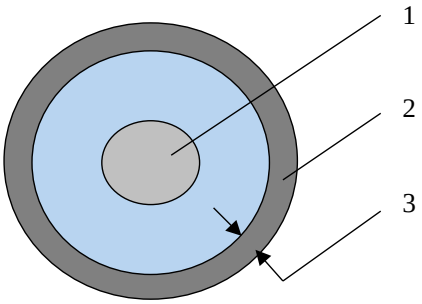
Обеспечение требуемого для автоматизированной системы управления (АСУ) уровня безопасности, его оценка и своевременное восстановление должно обеспечиваться набором соответствующих средств защиты, включающих не только средства перекрытия возможных каналов несанкционированного доступа (НСД), но и средства анализа объекта защиты на предмет выявления у него закладок (внутренние угрозы), производящих, как правило, нелегитимные действия в АСУ [1, с. 18], средства перекрытия каналов нелегитимного доступа (НЛД).

Предмет защиты помещен в замкнутую и однородную защитную оболочку, называемую преградой. Ценность предмета защиты не зависит от времени. Прочность защиты [2, с. 12] зависит от свойств преграды. Принципиальную роль играет способность преграды противостоять попыткам преодоления ее нарушителем. При этом для оценки защищенности информации используется свойство предмета защиты – способность привлекать его владельца и потенциального нарушителя.

В настоящее время известна модель элементарной защиты,

ориентированная на НСД [3, с. 52] (рис. 1).

Рисунок 1 – Модель элементарной защиты



1 – предмет защиты; 2 – преграда; 3 – прочность защиты

За условие достаточности защиты ($P_{сзи}$ = 1) принято превышение затрат времени на преодоление преграды нарушителем над временем жизни информации и отсутствие возможности обхода защиты [3, с. 61]. Данное условие отображено в виде выделенной ветви алгоритма принятия решения о достаточности защиты (рис. 2).

Здесь $P_{сзи}$ представляет собой вероятность не преодоления преграды нарушителем; $t_ж$ – время жизни информации; $t_н$ – ожидаемое время преодоления преграды нарушителем; $P_{обх}$ – вероятность обхода преграды нарушителем.

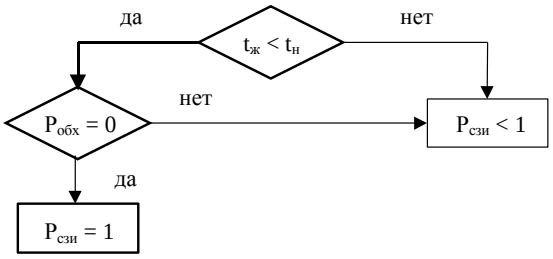


Рисунок 2 – Алгоритм принятия решения о достаточности защиты

При $P_{обх}$ = 0 преграда замкнута вокруг предмета защиты (рис. 2). Для реального случая, когда $t_ж > t_н$ и $P_{обх} > 0$, прочность защиты представлена в виде:

$$P_{сзи} = \min\left[(1 - P_{нр}), (1 - P_{обх})\right] \quad (1)$$

где $P_{нр}$ – вероятность преодоления преграды нарушителем за время, меньшее $t_ж$.

В случае же постоянно действующей преграды (защищаемая информация не устаревает или периодически обновляется) в формулу (1) вместо (1 – $P_{нр}$) вводится величина $P_{обл}$ – вероятность обнаружения и блокировки НСД [4, с. 30].

Особенностями известной модели элементарной защиты являются следующие положения:

1) определение в качестве нарушителя – физического лица;

2) перекрытие каналов несанкционированного доступа;

3) защита преградой от проникновения «снаружи».

Увеличение защитного свойства преграды предмета защиты – ее прочности осуществим за счет создания эшелонированной системы защиты [5, с. 77].

Рассмотрим в качестве предмета защиты некоторое программное средство, обрабатывающее и/или содержащее конфиденциальную или важную информацию. Исходя из специфики предмета защиты, под нарушителем будем понимать преимущественно искусственные объекты – программные закладки (ПЗ), ввиду их хороших маскировочных свойств и разрушающей способности по сравнению с нарушителем – физическим лицом [6, с. 102].

Проникновение ПЗ через преграду осуществляется в основном нелегитимным способом (нелегитимный доступ к предмету защиты). Понятие нелегитимного доступа D_L является обобщением понятия несанкционированного доступа D_S [7, с. 17] (рис. 3).

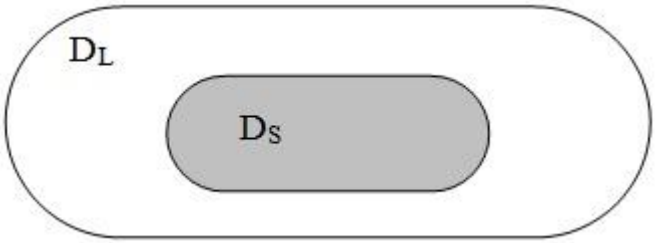


Рисунок 3 – Соотношение понятий доступа

Расширение понятия НСД подразумевает всего лишь нарушение принятой в системе политики безопасности, а исследования механизмов функционирования разрушающих программных средств (программных закладок) показали, что, как правило, ПЗ не нарушают правил разграничения доступа к информации. Под нелегитимными действиями программы или пользователя понимаются действия, наносящие ущерб безопасности или целостности системы (в нашем случае – предмету защиты). При этом все

нелегитимные действия включают несанкционированные с точки зрения политики безопасности и санкционированные, способные нарушить целостность и безопасность предмета защиты [8, с. 92].

Кроме «внешней» угрозы проникновения ПЗ к предмету защиты существует вероятность активизации ПЗ, размещенной в самом предмете защиты («внутренняя» угроза). При этом будем считать, что объектом воздействия ПЗ является объект, расположенный вне преграды от НСД. Эту особенность нарушителя, использующего в качестве исходной точки атаки предмет защиты, необходимо учитывать при проектировании преграды (системы защиты) и расчете ее прочности. Скорректированное фактическое значение вероятности преодоления преграды нарушителем ($P_ф$) в этом случае может быть рассчитано по формуле:

$$P_ф = 1 - (1 - P_1), (1 - P_2)] \qquad (2)$$

где $P_1 = P_{нр}$;

P_2 – вероятность появления «внутренней» угрозы.

Внутренние угрозы в расчетах можно исключить только в следующих ситуациях: когда преграда функционирует с самого начала жизненного цикла программного средства или программное средство прошло аттестацию по безопасности [9, с. 42].

Первое условие предполагает проектирование системы защиты параллельно с разработкой программного средства, т.е. предмета защиты. Невыполнение этого условия, «наложение» или «встраивание» системы защиты на этапе эксплуатации предмета защиты приводит к снижению прочности преграды, а также к большим временным затратам на учет дополнительных угроз.

Второе условие – аттестация программного средства. Процесс аттестации отличается от обычных испытаний более высоким уровнем формализации условий и результатов испытаний, проводимых специальным

подразделением [10, с. 22]. Документированным результатом аттестации является свидетельство о соответствии программного средства стандартам и другим нормативным актам.

Ограничением на модель элементарной защиты информации следует считать априорное принятие безопасным самой системы защиты.

Таким образом, распространяя имеющуюся модель элементарной защиты информации на особый тип нарушителя – ПЗ, прочность преграды можно увеличить, если добавить еще одно кольцо – преграду для защиты программного средства от санкционированного доступа (СД), способного привести к нарушению целостности и безопасности ПС (далее – преграда от НЛД). Полученная модель (рис. 4) характеризуется следующими дополнительными возможностями защиты:

1) обнаружение и блокировка каналов нелегитимного доступа к предмету защиты;
2) двусторонность защиты.

Совокупность двух преград представляет собой эшелонированную систему защиты от ПЗ. Причем преграда от НЛД, нарушающего целостность и безопасность ПС показана в виде двух колец: внешнего по отношению к ПС для защиты от внешних угроз и внутреннего (интегрированного с ПС) для защиты от внутренних угроз.

1 – предмет защиты – ПС; 2 – преграда от НЛД; 3 – преграда от НСД; 4 – прочность защиты

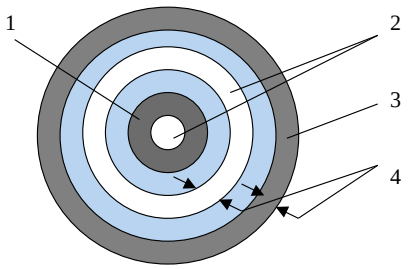


Рисунок 4 – Модель элементарной защиты программного средства

Отличие полученной модели от других типов моделей, приведенных в [11, с. 44] (модель многозвенной и многоуровневой защиты) состоит в следующем:

1) защита от двух различных типов доступов: НСД и СД, нарушающего целостность и безопасность предмета защиты, что приводит к невозможности объединения защиты от НСД и СД в один контур в качестве его отдельных звеньев;
2) отсутствие дублированных преград.

В качестве защиты от проникновения ПЗ может быть применена автоматизированная система обнаружения и блокировки ПЗ. Способность второй преграды (от НЛД, нарушающего целостность и безопасность ПС) обнаруживать и блокировать ПЗ должна учитываться при оценке ее прочности, аналогично первой преграде, путем введения в расчетную формулу величины $P_{пз}$ – вероятности обнаружения и блокировки программных закладок.

Принцип работы автоматизированной преграды защиты от ПЗ основан на непрерывном контроле поступающей информации к ПС. Поиск ПЗ проводится с помощью алгоритма распознавания, ориентированного на идентификацию ПЗ специального типа [11, с. 112]. Найденные отдельные «подозрительные» фрагменты информации формируют семантический образ закладки. Решение о заложенном в информацию разрушающем воздействии принимается человеком на основе методов нечеткой логики, что придает гибкость системе защиты от ПЗ. При этом необходимо дополнительное время на нейтрализацию ПЗ, включающее в себя как блокировку и запрещение доступа всей поступающей информации (закрытие канала доступа), так и блокировку отдельных управляющих воздействий (закрытие отдельных компонентов канала доступа).

Таким образом, условие прочности второй преграды с обнаружением и блокировкой ПЗ можно представить в виде соотношения:

(3)

где $t_п$ – время поиска ПЗ;

$t_{лок}$ – время локализации ПЗ;

$t_{реш}$ – время принятия решения о соответствии обнаруженной «подозрительной» информации ПЗ;

$t_{нт}$ – время нейтрализации ПЗ;

$t_{акт}$ – начало активизации разрушающей функции ПЗ;

t_1 – проникновение ПЗ;

$t_{акт} - t_1$ – период скрытого присутствия ПЗ.

Расчет прочности совокупности преград, включающей защиту от НСД и от НЛД, можно производить с использованием понятия нечеткого отношения на основе экспертных оценок $P_{обл}$, $P_{обх}$, $P_{пз}$. В этом случае формула (1) будет иметь следующий вид:

$$P_{сзи} = \min[\mu_R(U_{обл}, U_1), (1 - \mu_R(W_{обх}, W_{11}), (1 - \mu_R(W_{обх}, W_{1n}), \mu_R(U_{пз}, U_2), (1 - \mu_R(W_{обх}, W_{21}), (1 - \mu_R(W_{обх}, W_{2m})] \quad (4)$$

где R – нечеткое отношение «близко к»;

μ_R ( ) – функция принадлежности отношения R;

$U_{обл}$ и $U_{пз}$ – показатели, характеризующие способность преград к обнаружению и блокировке соответственно НСД и ПЗ;

U_1 и U_2 – максимальные показатели по обнаружению и

блокировке НСД и ПЗ;

$W_{обх}$ – показатель, характеризующий проникающую способность нарушителя (например, для физического лица – уровень технической оснащенности, для ПЗ – наличие и возможности функций внедрения и исследования);

W_1 и W_2 – показатели минимальной пропускающей способности i – го пути обхода соответственно первой и второй преграды;

n – число путей обхода первой преграды (от НСД);

m – число путей обхода второй преграды (от НЛД).

При этом увеличение прочности защиты ПС обусловлено уменьшением $Р_{отк}$ – вероятности отказа системы защиты. Формула итоговой прочности ($Ри_{сзи}$) полученной совокупности преград будет иметь следующий вид:

(5)

где $Р_{сзи}$ определяется с помощью формулы (4).

В результате можно сделать выводы о том, что принципы работы автоматизированной преграды защиты от ПЗ основан на непрерывном контроле поступающей информации. Решение, о заложенном в информацию разрушающем воздействии, принимается человеком на основе методов нечеткой логики, что придает гибкость системе защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Analysis of the aggressiveness of a software product / Khramov V.V., Trubnikov A.N. // Automatic Control and Computer Sciences. –1999. –Т. 33. – №2. – С. 28–34. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=13328155 (Дата обращения 12.02.2020 г.)

2. Алекперов И.Д. и др. Информационная безопасность и защита информации в цифровой экономике. Элементы теории и тестовые задания: Учебное пособие.– Южный университет (ИУБиП). – Ростов–на–Дону, 2020. – 114с. [Электронный ресурс]. – URL: https://www.elibra–ry.ru/item.asp?id=42393778 (дата обращения: 18.02.2020).
3. Доктрина информационной безопасности РФ (от 05.12.2016 года № 646), [Электронный ресурс]. – URL: http://docs.cntd.ru/document/420384668 (дата обращения 12.02.2020 г.).
4. Защита информации в вычислительных системах: Учебное пособие для вузов / Храмов В.В.,Садовов В.В., Трубников А.Н., Губарев О.К. – Москва, 2002.–192 с. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=32762286 (дата обращения 12.02.2020 г.).
5. Информационная безопасность и защита информации на транспорте: Тестовые задания по дисциплине / Голубенко Е.В., Ковтун О.Г., Храмов В.В. – Ростов–на–Дону, 2015. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp7idKJ6311930 (дата обращения 12.02.2020 г.).
6. Модель специальной программной закладки / Храмов В.В., Трубников А.Н. // Вопросы защиты информации. –1998. –№1–2 (40–41). – С. 36–37. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp7idK36309954 (дата обращения 12.02.2020 г.).
7. Основы методологии синтеза средств защиты информации / Храмов В.В. // Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем: Материалы XXI Межведомственной научно–технической конференции. –2002.– С. 115–120. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp7idKJ2877301 (Дата обращения 12.12.2019г.) (дата обращения 12.02.2020 г.).
8. Способ повышения безопасности программных средств и пути его реализации / Губарев О.К.,Храмов В.В. // Тематический научно–технический сборник. – Пущино, Научный Центр РАН, 1994. –С. 56–61. – URL: https://elibrary.ru/item.asp/ (дата обращения 12.12.2019 г.)
9. Стратегия национальной безопасности РФ (Указ Президента РФ от 31 декабря 2015 г. N 683), [Электронный ресурс]. – URL: http://base.garant.ru/71296054/ (Дата обращения 12.02.2020 г.).
10. Федеральный закон «О безопасности» (от 28.12.2010 N 390–ФЗ) [Электронный ресурс]. – URL: https://legalacts.ru/doc/federalnyi–zakon–ot–28122010–п–390–&–о/ (дата обращения 12.02.2020 г.).
11. Храмов В.В. и др. Защита информации в вычислительных системах: учебное пособие для вузов. – М., 2002.–192с. – URL:https://elibrary.ru/item.asp?id=32762286 (дата обращения: 18.01.2020).