В. В. Грызунов (к. т. н.)
Военно-космическая академия имени А. Ф. Можайского

БЕЗОПАСНОСТЬ В ЦЕЛОСТНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

На любом предприятии информационная система (ИС) является стратегически и тактически важным объектом, так как от ее работоспособности зависят полнота и целесообразность использования ресурсов предприятия. Можно сказать, что с помощью ИС координируются и согласуются действия других элементов предприятия, контролируется использование и распределяются ресурсы предприятия. Именно поэтому контроль над ИС является основной целью злоумышленников [1]. Обеспечение безопасности ИС позволяет гарантировать использование ресурсов предприятия в интересах его владельцев, а не в интересах злоумышленников, получивших несанкционированный доступ к ИС. Обеспечение безопасности ИС имеет ряд особенностей, присущих ИС как иерархической системе.

ИС представляет собой сложный объект, имеющий несколько уровней иерархии. Условно эти уровни можно представить так, как это показано на рис. 1. Распространим утверждения, приведенные в [2], на ИС. Можно сказать, что каждый вышестоящий уровень является «метасистемой» для всех нижестоящих уровней, т. е. «аксиомой», задающей основные требования к множеству допустимых и необходимых пространственно-временных состояний нижестоящих уровней. «Аксиомой, не требующей доказательств», для программного обеспечения (ПО) является аппаратное обеспечение (АО), для аппаратного обеспечения — действия персонала (П). Персонал, в свою очередь, должен действовать в соответствии с условиями и ограничениями различных видов обеспечения (об).

Так, например, ПО, выполняясь, использует предоставленную процессором систему команд и может получить доступ только в те участки памяти, что разрешены процессором, а современные процессоры выделяют область памяти, куда запрещают доступ для всех программ. Само аппаратное обеспечение (и, соответственно, ПО) функционирует под управлением персонала, который подает электропитание, разграничивает доступ к оборудованию и т. д.

Говоря про персонал, необходимо отметить, что человек по своей природе — биосоциальное существо, обладающее психикой. Соответственно, на него влияют как законы реального мира, так и нормы морали, юридические законы, экономические и психологические факторы и т. п. Разные факторы влияют на разных людей по-разному. Например, неправомерный доступ к компьютерной информации или распространение вредоносных программ запрещено Уголовным кодексом. Однако сильная нужда, тщеславие или жадность могут сделать более приоритетным получение экономической выгоды, и человек пойдет на преступление. Или, например, введенный в состояние «зомби» человек будет беспрекословно выполнять инструкции злоумышленника. Человек — пока не изученное существо, и классификация элементов обеспечивающего уровня — предмет дополнительных исследований, поэтому далее, говоря об обеспечивающем уровне, будем иметь в виду лишь явно выделяющиеся нормативно-правовую, экономическую и психологическую составляющие.

Для обеспечения безопасности каждый уровень должен представлять собой *целостную* систему [3, 4]. Это означает, что должно выполняться условие

$$\int_{Q^{У}} \varphi^{У}(r^{У})\,dr^{У} = I^{У}, \qquad (1)$$

где $Q^{У}$ — множество требуемых состояний уровня ИС; $r^{У} \in Q^{У}$; $I^{У}$ — показатель эффективности применения уровня ИС; $\varphi^{У}(r^{У})$ — способность уровня решать поставленные задачи в состоянии $r^{У}$ (по сути, производительность уровня в состоянии $r^{У}$); У = об, П, АО, ПО.

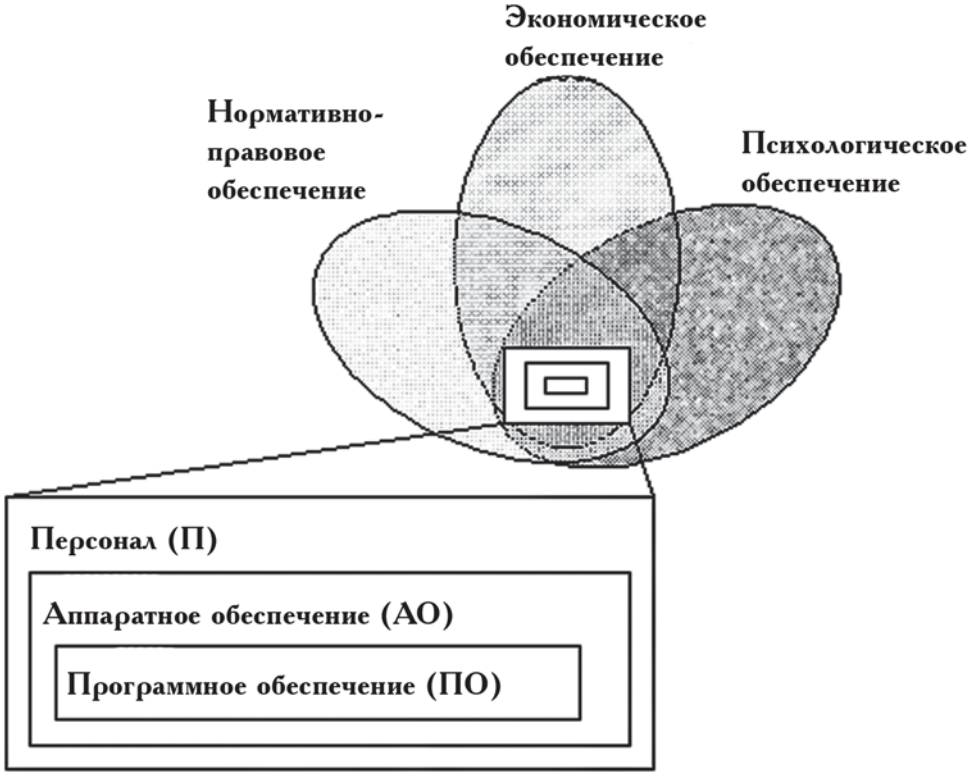

Рис. 1. Уровни иерархии ИС

Поскольку работоспособность верхних уровней зависит от работоспособности нижних уровней $\varphi^{ИС}(r^{ИС}) = \varphi^{об}(r^{об}, \varphi^{П}(r^{П}, \varphi^{АО}(r^{АО}, \varphi^{ПО}(r^{ПО}))))$ то связь эффективностей применения ИС различных уровней и множеств требуемых состояний уровней можно записать следующим образом:

$$\int_{Q^{об}} \int_{Q^{П}} \int_{Q^{АО}} \int_{Q^{ПО}} \varphi^{ИС}(r^{ИУС}) dr^{ПО} dr^{АО} dr, ^{П} dr^{об} = I^{ИС} \quad (2)$$

при этом

$Q^{об} \cup Q^{П} \cup Q^{АО} \cup Q^{ПО} = Q^{ИС}$,

поэтому с учетом (1) верно

$I^{об}(I^{П}(I^{АО}(I^{ПО}))) = I^{ИС}$, (3)

где $Q^{об}$, $Q^{П}$, $Q^{АО}$, $Q^{ПО}$, $Q^{ИС}$ — соответственно множества требуемых состояний обеспечивающего уровня, персонала, аппаратного и программного обеспечений, всей ИС; $r \in Q^{ИС}$; $I^{об}$, $I^{П}$, $I^{АО}$, $I^{ПО}$, $I^{ИС}$ — соответственно эффективности применения обеспечивающего уровня, персонала, аппаратного и программного обеспечений, всей ИС; $\varphi^{ИС}(r^{ИС})$ — способность ИС решать поставленные задачи в состоянии $r^{ИС}$.

Если для объекта верно равенство (2), говорят, что *объект обладает целостностью*.

В свою очередь, верхние уровни определяют, на что именно в их работе влияет и как будет учитываться эффективность применения нижнего уровня. Это решается при задании функции $\varphi^{У}$. Определяя функцию $\varphi^{У}$, верхний уровень накладывает ограничения (предъявляет требования) на множества требуемых состояний нижних уровней.

Из выражений (2) и (3) видно, что нижние уровни влияют на верхние посредством формирования своего показателя эффективности применения. Уровень может *непосредственно* взаимодействовать только с уровнем, ближайшим к нему. Это хорошо заметно при взаимодействии уровней «персонал» и «ПО». Человек не может непосредственно воздействовать на ПО, для этого ему нужно АО (клавиатура, мышь, стилус и т. д.). И, наоборот, ПО не может непосредственно передавать человеку результаты обработки данных без средств отображения информации (мониторов, принтеров, виртуальных шлемов и т. д.).

Обобщая изложенное, можно сказать, что каждый уровень служит неким буфером, преобразующим свойства (ограничения, требования) верхнего уровня в свои и свойства (ограничения, требования) нижнего уровня.

Проиллюстрируем взаимодействие уровней. Нормативно-правовое обеспечение накладывает свои ограничения в виде требований нормативно-правовых актов. Например, для обеспечения безопасности информации в ИС исполнительных органов государственной власти необходимо использовать аппаратное и программное обеспечение, прошедшее специальные проверки во ФСТЭК России или ФСБ [5, 6], персонал должен пройти соответствующую подготовку [7]. При этом на создание ИС и оплату персонала не может быть потрачено больше средств, чем запланировано в бюджете (ограничение экономического обеспечения). Рассматривая детально подобным образом все элементы обеспечивающего уровня, можно сформулировать требования к нижним уровням.

Требования, сформулированные на обеспечивающем уровне, могут быть реализованы только персоналом. Персонал, в свою очередь, выдвигает требования к нижестоящим уровням. Допустим, персонал в высшем учебном заведении активно изучал платформу Intel и операционную систему Windows. Естественно, что потом в своей работе персонал будет ориентироваться именно на известные ему технологии. Обозначенное АО (платформа Intel) имеет такие особенности, как, например, наличие процессоров Xeon со своей системой команд, объем доступной оперативной памяти и т. д. Это выдвигает свои требования к уровню «ПО», например: операционная система Solaris, Linux или Windows. Персонал, естественно, выберет Windows, что сделает возможным применение Active Directory, MS Office и т. д. В итоге требования, предъявляемые всеми уровнями ИС, формируют множество допустимых состояний ИС ($R^{ИС}$), содержащее множество требуемых состояний ИС ($Q^{ИС}$)

$$r^{ИС} \in Q^{ИС} \subset R^{ИС}.$$

Связь с вышестоящими уровнями реализуется через показатель эффективности применения уровня ($I^{У}$). Например, существует большое количество мобильных пользователей ИС, работающих с операционными системами, отличными от семейства Windows. Это не позволяет авторизовать их в Active Directory с требуемой достоверностью. Такое обстоятельство мешает всей ИС в полном объеме достичь целей своего применения. Однако любая система может достичь целей своего применения путем качественного изменения своих пространственно-временных состояний $R^{ИС}$ [3, 4]. Для этого корректируются требования вышестоящих уровней. *Корректировка производится от нижних уровней к верхним*. Так, в приведенном примере возможно использовать eDirectory вместо Active Directory, это потребует заменить Windows на Solaris. Изменение свойств ПО может повлечь за собой изменение свойств АО, например смена Intel на SPARC. Новые свойства ПО и АО корректируют требования к персоналу, что, как правило, влечет за собой внесение поправок в бюджет и/или нормативно-правовое обеспечение.

Рассмотрим, каким образом необходимо обеспечивать безопасность информации в ИС как в иерархической системе.

Здесь важно помнить, что основная задача злоумышленника состоит в том, чтобы заставить атакуемую систему работать в своих интересах [1]. Атакуя в пределах одного уровня, злоумышленник может корректировать только производительность атакуемого уровня ИС ($\varphi^{У}$). Если уровень обладает целостностью (1), то изменение пространства требуемых состояний уровня средствами самого уровня невозможно, так как это пространство формируется вышестоящими уровнями (метасистемой) на этапе создания уровня. Изменение производительности уровня отражается на всех вышестоящих уровнях, поскольку изменяется показатель эффективности применения уровня (см. выражение (3))

$$\int_{Q^{У}} \Delta\varphi^{У}(r^{У})dr^{У} \Rightarrow \Delta I^{У}.$$

Более подробно взаимодействие злоумышленника и информационной системы в рамках одного уровня рассмотрено в [8].

В этом случае в ИС, обладающей целостностью, при достаточном количестве доступных ИС ресурсов атака обнаруживается, локализуется и нейтрализуется. Соответственно, злоумышленнику довольно сложно реализовать свои интересы. Совсем иначе обстоит дело, если уровень атакуется средствами вышестоящих уровней. Здесь злоумышленник может воздействовать как на пространство требуемых состояний атакуемого уровня ($Q^У$), так и на его производительность ($\varphi^У$). Тогда задача злоумышленника сводится к тому, чтобы подобрать такие изменения $Q^У$ и $\varphi^У$, чтобы $I^У$ достиг требуемого злоумышленнику значения либо остался неизменным, т. е.

$$\Delta Q^У, \Delta\varphi^У : (I^У \to I^{треб\ зл.}\ или \Delta I^У \to 0).$$

В случае с неизменным $I^У$ атака не будет обнаружена. Однако стоит отметить, что изменение $Q^У$ и $I^У$ какого-то уровня возможно только путем изменения $Q^У$ и $I^У$ вышестоящего уровня, а изменение $Q^У$ и $I^У$ вышестоящего уровня потребует изменения $Q^У$ и $I^У$ еще более вышестоящего уровня и т. д. Следовательно, если в ИС *все* уровни обладают целостностью, то проведение атаки становится невозможным (при наличии необходимых ресурсов). Либо злоумышленник должен подняться вверх до такого уровня, где целостность не проверяется, а это, согласно теореме Гёделя о неполноте [2], вполне возможно.

Проиллюстрируем сказанное на примере ИС Государственного Заказа Санкт-Петербурга. Допустим, злоумышленнику необходимо подделать электронный документ, содержащий наименование предприятия, победившего в электронных торгах. В ИС передаваемые электронные документы проходят проверку целостности посредством формирования электронно-цифровой подписи (ЭЦП). Соответственно, непосредственные изменения документа будут обнаружены. Проверку целостности производит сертифицированное во ФСТЭК и ФСБ средство криптографической защиты информации (СКЗИ). Т. е. вероятность появления в СКЗИ недокументированных возможностей (изменение злоумышленником $Q^{ПО}$ для СКЗИ) чрезвычайно мала. Более того, данное СКЗИ само контролирует свою целостность, т. е. внедрение в СКЗИ несанкционированных алгоритмов практически невозможно. Следовательно, при условии целостности операционной системы (выполнение для операционной системы (1)) средствами уровня «ПО» задачу по подделыванию электронных документов не решить.

На уровне «АО» атака может быть реализована путем копирования носителей, содержащих закрытые ключи пользователей, после чего модифицированный электронный документ может быть подписан ЭЦП от имени легитимного пользователя. В этом случае СКЗИ отработает в соответствии со своим Q, уже измененным на вышестоящем уровне «АО», сформирует ожидаемый от нее результат, и атака будет успешной. Другой сценарий может состоять в том, чтобы изменить устройство отображения результатов работы СЗКИ. СКЗИ сформирует ошибку, но персонал этого не увидит. Однако если в ИС существует жесткий регламент работы с ключевыми носителями, в котором запрещено копирование ключевых носителей и организован их строжайший учет, разграничен физический доступ к АО, то реализация описанной атаки на уровне «АО» станет проблематичной.

Реализация регламента работы с ключевыми носителями (нормативно-правовая составляющая уровня «об») возлагается на персонал (уровень «П»). Поэтому, перенеся атаку на уровень «П», злоумышленник должен заинтересовать персонал в том, чтобы нарушить регламент и предоставить ключевой носитель для копирования либо «закрыть глаза» на сообщения СКЗИ о том, что проверяемый документ изменен после подписания.

Предположим, что и здесь злоумышленника ждет неудача, так как персонал морально устойчив и материально обеспечен. Злоумышленник вынужден подниматься на уровень «об» и производить воздействие здесь. Такое воздействие может заключаться, например, во внесении в регламент изменений, разрешающих копирование ключевых носителей, ослабляющих контроль над доступом к «АО», либо в изменении нормативно-правовых актов в сторону разрешения к использованию несертифицированных СКЗИ, либо в урезании финансирования, скажем, с целью снижения качества персонала, и т. п.

Как видно, чем выше уровень, на который воздействует нарушитель, тем больше возможностей по корректировке $Q^{ИС}$ он имеет. Противостоять этому возможно только путем контроля целостности каждого уровня ИС и целостности связей между уровнями (выражения (1), (2) и (3)). Названные выражения *формализуют* базовую закономерность — *целостность информационной системы* и позволяют, применяя готовые математические аппараты, изучать свойства информационной системы.

Таким образом, для обеспечения безопасности информации в информационной системе *необходимо и достаточно обеспечить целостность всех уровней ИС* и реализовать связь между ними как от вышестоящих к нижестоящим, так и, наоборот, от нижестоящих к вышестоящим.

СПИСОК ЛИТЕРАТУРЫ:

1. *Расторгуев С. П.* Информационная война. М., 1998. — 416 с.
2. Теоремы Гёделя о неполноте http://ru.wikipedia.org/wiki.
3. *Бурлов В. Г.* Синтез модели вычислений в условиях разрушаемой программно-аппаратной среды // Сборник алгоритмов и типовых задач. № 20 / Под ред. И. А. Кулешова. СПб., 2002. С. 220–235.
4. *Бурлов В. Г.* Основы моделирования социально-экономических и политических процессов (Методология. Методы.). СПб., 2007. — 267 с.
5. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».
6. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
7. Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».
8. *Грызунов В. В.* Структурно-функциональный синтез модели системы предотвращения вторжений // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 31–38.

В. А. Минаев[1] *(д. т. н., профессор)*
Российский новый университет (проректор),
В. П. Хренов[2]
Российский новый университет (заместитель директора Института систем и технологий безопасности)

ФУНДАМЕНТАЛЬНАЯ ЗАКОНОМЕРНОСТЬ ФОРМИРОВАНИЯ ПРОСТЫХ ЧИСЕЛ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В последовательности простых чисел есть
тайна, непостижимая человеком.
Л. Эйлер

Работа посвящена математическому доказательству фундаментального закона формирования простых (первых) чисел. Описаны соотношения формирования составных чисел. Представлена новая структура натурального ряда чисел, рассмотрены прикладные аспекты открытия, в том числе в области прикладной математики, информационной безопасности, педагогики.

[1] *В. А. Минаев — автор ряда формализаций при математическом обосновании закономерности формирования натурального ряда чисел и описания прикладных аспектов открытия.*
[2] *В. П. Хренов — автор открытия закономерности формирования натурального ряда.*