М.М. Бусько

БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Методические указания по выполнению практических работ

Министерство науки и высшего образования Российской Федерации
Байкальский государственный университет

М.М. Бусько

БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Методические указания по выполнению практических работ

Иркутск
Научное издательство БГУ
2020

УДК 004.056.53
ББК 018.2*32.973я73
Б92

Печатается по решению редакционно-издательского совета
Байкальского государственного университета

Рецензент канд. экон. наук, доц. З.В. Архипова

Бусько, М.М.
Б92 Безопасность и защита информации : метод. указания по выполнению практ. работ / М.М. Бусько. — Иркутск : Науч. изд-во БГУ, 2020. — 48 с. — Текст : электрон.

Методические указания по выполнению практических работ подготовлены в соответствии с программой учебного курса «Безопасность и защита информации». Описание каждой практической работы сопровождается краткими теоретическими сведениями, заданиями и контрольными вопросами для проверки теоретических знаний.

Предназначено для студентов, обучающихся по направлению подготовки магистратуры 09.04.03 «Прикладная информатика» очной и заочной форм обучения.

УДК 004.056.53
ББК 018.2*32.973я73

Оглавление

Предисловие

Дисциплина «Безопасность и защита информации» входит в обязательную часть учебного плана направления подготовки магистратуры 09.04.03 Прикладная информатика. Основное назначение данной дисциплины состоит в эффективном освоении основ теории информационной безопасности, элементов формальной теории защиты информации, а также основных оценочных и управленческих подходов в области информационной безопасности.

Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности. Универсальных методов защиты не существует, во многом успех при построении механизмов безопасности для реальной системы будет зависеть от ее индивидуальных особенностей. Однако за практическими приемами построения систем защиты лежат общие закономерности, которые не зависят от технических особенностей их реализации. Такие универсальные принципы и составляют теоретические основы информационной безопасности, ее формализованное представление.

Теоретический базис информационной безопасности позволяет адекватно описывать процессы в условиях неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз). Высокая степень формализации вводит понятие модели защиты информации, описывает доказательный подход в построении систем защиты, позволяющий принимать решение о гарантированно защищенных системах обработки информации.

Настоящие методические указания по выполнению практических работ как раз и предназначены для закрепления теоретических знаний по формальной теории защиты информации.

Тематика практических работ полностью соответствует рабочей программе курса, их количество согласно учебному плану.

Описание каждой практической работы сопровождается краткими теоретическими сведениями, заданием и контрольными вопросами по проверке теоретических знаний.

Практическая работа № 1

Менеджмент риска информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010

Цель работы: ознакомиться с алгоритмами оценки риска информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010.

Основные определения

Уязвимость (vulnerability): Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами. (ГОСТ Р ИСО/МЭК 27002-2012).

Угроза (threat): Потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации. (ГОСТ Р ИСО/МЭК 27002-2012).

Актив (asset): Все, что имеет ценность для организации (ГОСТ Р ИСО/МЭК 27002-2012).

Риск (risk): Сочетание вероятности события и его последствий (ГОСТ Р ИСО/МЭК 27002-2010).

Риск информационной безопасности (information security risk): Возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Примечание. Он измеряется исходя из комбинации вероятности события и его последствия.

(ГОСТ Р ИСО/МЭК 27005-2010).

Теоретические сведения

Риск представляет собой комбинацию последствий, вытекающих из нежелательного события и вероятности возникновения события. Оценка риска количественно или качественно характеризует риски и дает возможность руководителям назначать для них приоритеты в соответствии с осознаваемой ими серьезностью или другими установленными критериями.

В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры и средства контроля и управления и их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование по критериям оценки риска, зафиксированным при установлении контекста.

Активом является что-либо, имеющее ценность для организации и, следовательно, нуждающееся в защите. При определении активов следует иметь в виду, что информационная система состоит не только из аппаратных и программных средств.

Существует много типов активов, включающих:

a) информацию: базы данных и файлы данных, договоры и соглашения, системная документация, исследовательская информация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки, планы непрерывности бизнеса, меры по переходу на аварийный режим, контрольные записи и архивированная информация;

b) программные активы: прикладные программные средства, системные программные средства, средства разработки и утилиты;

c) физические активы: компьютерное оборудование, средства связи, съемные носители информации и другое оборудование;

d) услуги: вычислительные услуги и услуги связи, основные поддерживающие услуги, например, отопление, освещение, электроэнергия и кондиционирование воздуха;

e) персонал, его квалификация, навыки и опыт;

f) нематериальные ценности, например, репутация и имидж организации.

Угроза может причинить ущерб активам организации, таким как информация, процессы и системы. Угрозы могут возникать в результате природных явлений или действий людей, они могут быть случайными или умышленными. Должны быть установлены и случайные, и преднамеренные источники угроз. Угрозы могут проистекать как из самой организации, так и из источника вне ее пределов. Угрозы должны определяться в общем и по виду (например, неавторизованные действия, физический ущерб, технические сбои), а затем, где это уместно, отдельные угрозы определяются внутри родового класса. Это означает, что ни одна угроза, включая неожиданные угрозы, не будет упущена, но объем требуемой работы, несмотря на это, сокращается.

Некоторые угрозы могут влиять более чем на один актив. В таких случаях они могут быть причиной различных влияний в зависимости от того, на какие активы оказывается воздействие.

Наличие уязвимости само по себе не наносит ущерба, поскольку необходимо наличие угрозы, которая сможет воспользоваться ею. Для уязвимости, которой не соответствует определенная угроза, может не потребоваться внедрение средства контроля и управления, но она должна осознаваться и подвергаться мониторингу на предмет изменений. Следует отметить, что неверно реализованное, неправильно функционирующее или неправильно используемое средство контроля и управления само может стать уязвимостью. Меры и средства контроля и управления могут быть эффективными или неэффективными в зависимости от среды, в которой они функционируют. С другой стороны, угроза, которой не соответствует определенная уязвимость, может не приводить к риску.

Уязвимости могут быть связаны со свойствами актива. Способ и цели использования актива могут отличаться от планируемых при приобретении или создании актива. Необходимо учитывать уязвимости, возникающие из разных источников, например, те, которые являются внешними или внутренними по отношению к активу.

Последствия для активов, вызванные потерей конфиденциальности, целостности и доступности могут быть обусловлены сценарием инцидента. Сценарий инцидента — это описание угрозы, использующей определенную уязвимость или совокупность уязвимостей в инциденте ИБ. Влияние сценариев инцидентов обусловливается критериями влияния, определяемыми в течение деятельности по установлению контекста. Влияние может затрагивать один или несколько активов, а также часть актива. Поэтому активам может назначаться ценность, обусловленная как их финансовой стоимостью, так и последствиями для бизнеса в случае их порчи или компрометации. Последствия могут быть временными или постоянными, как это бывает в случае разрушения активов.

Установление значения риска может быть качественной оценкой, количественной или комбинированной, в зависимости от обстоятельств. На практике установление качественного значения часто используется вначале для получения общих сведений об уровне риска и выявления основных значений рисков. Позднее может возникнуть необходимость в осуществлении более специфичного установления количественного анализа основных значений рисков, поскольку обычно выполнение качественного анализа по сравнению с количественным является менее сложным и затратным.

Для установления качественного значения используется шкала квалификации атрибутов, с помощью которой описываются величины возможных последствий (например, низкий, средний и высокий) и вероятности возникновения этих последствий. Преимущество установления качественного значения заключается в доступности для понимания всем соответствующим персоналом, а недостатком — зависимость от субъективного выбора шкалы.

Для установления количественной оценки используется шкала с числовыми значениями (а не описательные шкалы, используемые при установлении качественного значения) как последствий, так и вероятности, с применением данных из различных источников. Качество анализа зависит от точности и полноты числовых значений и от обоснованности используемых моделей. В большинстве случаев для установления количественного значения используются фактические данные за прошедший период. Преимущество заключается в том, что установление количественного значения может быть напрямую связано с целями информационной безопасности и проблемами организации. Недостатки количественного подхода могут иметь место, когда фактические проверяемые данные недоступны, поэтому создается иллюзия ценности и точности установления количественного значения риска.

Порядок выполнения работы

Подготовительным этапом выполнения практической работы является определение объекта защиты (объекта информатизации). В качестве такого объекта может выступать организация (предприятие), с которым студент хорошо знаком по роду своей деятельности или предыдущему опыту и представляющий

для него интерес. Это может быть место работы студента, организация знакомая ему по учебной и производственной практике.

При выборе объекта работ следует учитывать: интересы студента к проблеме в той или иной области; степень личного знакомства с намечаемым для изучения объектом; характер и объем практически доступных для использования источников и материалов, описывающих предметную область.

Основным объектом защиты должна выбираться информационная система предприятия. При этом под ней подразумевается совокупность базы данных предприятия, программы-оболочки, используемой для работы с ней, серверов, на которых расположена база, АРМ пользователей, коммуникационного оборудования, линий связи, дополнительного оборудования (принтеров, сканеров и т.п.).

Задания

1. Воспользуйтесь справочной правовой системой «КонсультантПлюс» и ознакомьтесь с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

2. Определите перечень типов информационных активов для своего объекта информатизации.

3. Установите ценность активов для своего объекта информатизации в соответствии с примерами, рассматриваемыми в **Приложении B** стандарта ГОСТ Р ИСО/МЭК 27005-2010.

4. Из **Приложения D** ГОСТа выберите актуальные уязвимости системы защиты тех информационных активов, которые были определены и оценены в пп. 2–3.

5. Пользуясь **Приложением C** ГОСТа определите угрозы, реализация которых возможна пока в системе не устранены имеющиеся уязвимости.

6. Пользуясь методами, предложенными в **Приложении E** ГОСТа, произведите оценку рисков информационной безопасности.

Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

7. Полученные результаты необходимо представить в виде отчета.

Контрольные вопросы

1. Раскрыть сущность комплексной системы защиты информационных активов предприятий.

2. Раскрыть особенности система защиты информационных активов хозяйствующего субъекта.

3. Исследовать особенности организационного направления в деятельности по защите информационных активов предприятия.

4. Охарактеризовать сущность направления в организационной защите — работе с персоналом, определении его надежности.

5. Как осуществить оценку надежности персонала как основного источника угроз информационным активам предприятия?

6. Суть методики оценки возможного ущерба при реализации угроз безопасности.

7. Охарактеризовать сущность направления в организационной защите — информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.

8. Обосновать позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.

9. Какова взаимосвязь понятий «информационных активов» и «системы оценки рисков информационной безопасности хозяйствующего субъекта»?

Практическая работа № 2

Определение оценки вероятности реализации угроз

Цель работы — ознакомиться с методикой подсчета оценки вероятности реализации угроз и критериями эффективности.

Теоретические сведения

Оценка вероятности реализации угроз

Любая возможность характеризуется вероятностью ее реализации. Эта вероятность P зависит от вероятности выполнения соответствующего действия $P_Д$ и вероятности отсутствия противодействия, а именно:

$$P = P_Д \cdot Q_П. \quad (1)$$

где $P_Д$ — вероятности выполнения соответствующего действия (угрозы); $Q_П$ — вероятности отсутствия противодействия (угрозе).

Если противодействия нет ($Q_П$ = 1), то вероятность реализации угрозы определяется только вероятностью выполнения соответствующего действия. Если противодействие угрозе есть и оно абсолютно эффективно ($Q_П$ = 0), реализация угрозы невозможна (ее вероятность P = 0).

Рассмотрим возможные сценарии и сделаем следующие выводы:

1. Вероятность того, что будет предпринято действие по реализации угрозы определяется вероятностью совпадения двух факторов: 1) должен появиться субъект определенного класса (вероятность P_C); 2) этот субъект должен «выбрать» соответствующий вид угрозы (вероятность $P_{ВУ}$ выбора угрозы).

Вероятность совпадения этих факторов (вероятность выполнения угрозы) равна произведению вероятностей, т.е.

$$P_Д = P_C \cdot P_{ВУ}\,. \quad (2)$$

2. Если некоторый вид угрозы может осуществляться несколькими субъектами, то вероятность действия будет равна сумме вероятностей вида (2):

$$P_Д = P_{C1} \cdot P_{ВУ1} + P_{C2} \cdot P_{ВУ2} + \ldots + P_{Cn} \cdot P_{ВУn}\,. \quad (3)$$

В общем виде равенство (3) можно записать в форме:

$$P_Д(j) = \sum_{i=1}^{n} P_i p(j/i),\ j = 1,2,...,m\,, \quad (4)$$

где $P_Д(j)$ — вероятность попытки реализации угрозы j-го типа; P_i — вероятность появления субъекта i-го типа; $p(j/i)$ — условная вероятность того, что субъект i-го типа выберет для реализации угрозу j-го типа; n — число типов субъектов; m — число типов угроз.

Значения всех вероятностей лежат в пределах от нуля до единицы. Каждый случай, когда сумма вероятностей вида (4) превышает единицу, должен анализироваться на содержательном уровне.

3. Как видно из равенства (1), вероятность реализации P уменьшается с уменьшением $Q_П$. Поскольку вероятность отсутствия противодействия $Q_П$ связана с вероятностью противодействия $P_{ПД}$ равенством $Q_П + P_{ПД} = 1$, то, очевидно, для уменьшения P следует увеличивать вероятность противодействия угрозам. Противодействие может быть направлено: 1) на конкретный тип субъекта; 2) на

защиту от определенного вида угрозы. Обозначим вероятность отсутствия противодействия i-му субъекту при реализации j-й угрозы q_{ij} и запишем соотношение (4) в форме:

$$P_Д(j) = \sum_{i=1}^{n} P_i p(i/j) q_{ij} = \sum P_i p(j/i)(1 - p_{ij}) . \quad (5)$$

Видно, что в случае отсутствия противодействия или (q_{ij} = 1 или p_{ij} = 0) формула (5) переходит в (4).

Общее уравнение оценки вероятности реализации угрозы (1) содержит две составляющие: вероятность действия $P_Д$ и вероятность отсутствия противодействия $Q_П$.

Первая составляющая описывается равенством (5).

Рассмотрим вторую составляющую $Q_П$. Для ее оценки обратимся к рис. 1, где символами «+» и «–» отмечены успех и неуспех системы защиты, а символами A, B, C и D — средства защиты.

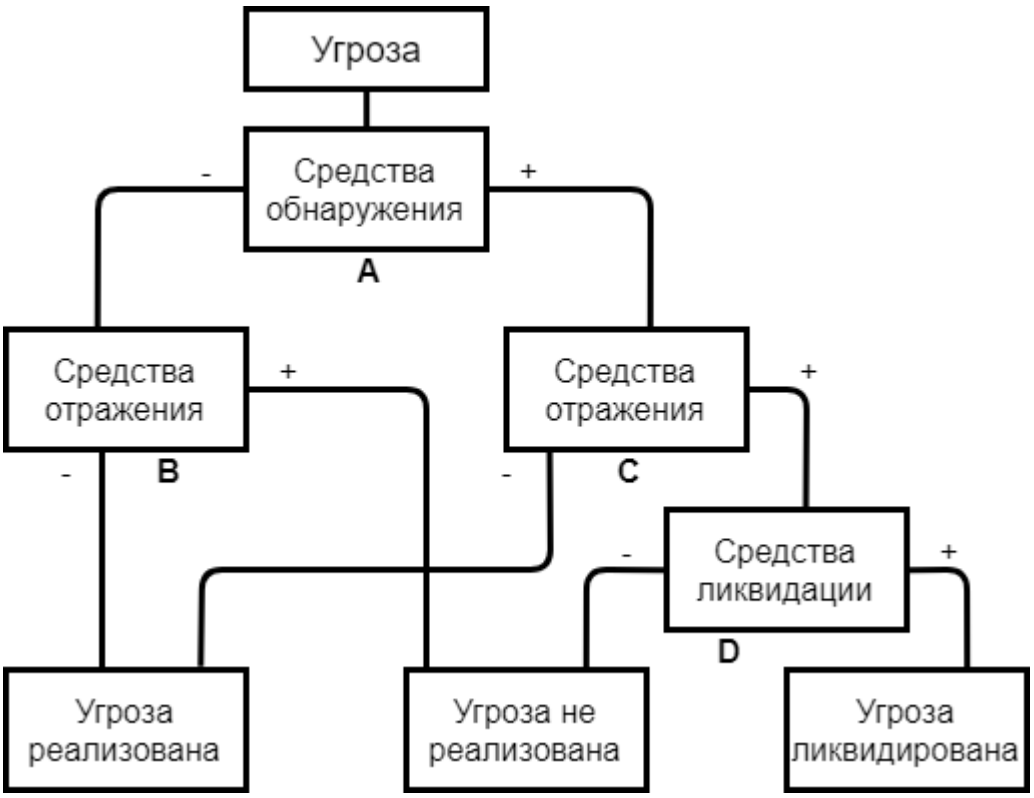


Рис. 1. Противодействие угрозам

Случаю отсутствия противодействия соответствует путь A^-B^- на рис. 1. Его вероятность $Q_П = p(A^-) \cdot p(B^-) = q_1 \cdot q_2$. Вероятность того, что система или средства обнаружения не обнаружили субъект угрозы или угрозу, зависит от режима функционирования и от правильности срабатывания (надежности, конструктивных особенностей и т.п.).

Для простоты будем рассматривать средства обнаружения непрерывного действия. Тогда вероятность q_1 будет определяться последним фактором: $q_1 = q_{н1}$,

где $q_{н1}$ — вероятность несрабатывания средств обнаружения. Если средств обнаружения нет, то $q_1 = 1$.

Вероятность q_2 преодоления средства отражения, в первую очередь зависит от того, каким временем располагает субъект угрозы: если это время $t_{от} = 0$, то угроза не реализуется; если время t от бесконечно, то угроза реализуется. Такая зависимость q_2 от времени представляется экспоненциальной функцией

$$y(t) = 1 - \exp(-\alpha t),$$

где α — постоянная величина, характеризующая «скорость» реализации угрозы.

Если система отражения неисправна (вероятность $q_{н2}$) или вообще отсутствует ($q_{н2} = 1$), то субъекту угрозы для ее преодоления не требуется специальных усилий и средств, связанных с затратой времени преодоления отражения $t_{от}$. Следовательно,

$$q_2 = q_{н2} + [1 - \exp(-\alpha t_{от})](1 - q_{н2})$$

Окончательно получаем:

$$Q_{П} = q_{н1}(q_{н2} + [1 - \exp(-\alpha t_{от})](1 - q_{н2})),$$

Проверкой убеждаемся в справедливости оценок для частных случаев:

1. $A^- B^-$ — защиты нет: $q_{н1} = 1$, $q_{н2} = 1$. Тогда $Q_{П} = 1$, т.е. преодоление рубежа абсолютно возможно.

2. $A^- B^+$ — средств обнаружения нет, средства отражения абсолютно эффективны: $q_{н1} = 1$, $q_{н2} = 0$. Тогда $Q_{П} = 1 - \exp(-\alpha t_{от})$. Если злоумышленник не располагает временем на преодоление ($t_{от} = 0$), то $Q_{П} = 0$, т.е. преодоление защиты абсолютно невозможно.

Возвращаясь к соотношению (1) и учитывая (5), запишем общую вероятность реализации угрозы j-го типа в виде:

$$P_{Д}(j) = \sum_{i=1}^{n} P_i \, p(j/i) q_{н1}(q_{н2} + [1 - \exp(-\alpha t_{от i})](1 - q_{н2})), \qquad (6)$$

где индекс i обозначает субъект i-го типа.

Общая вероятность нарушения безопасности объекта при принятых допущениях запишется в форме:

$$P(j) = \sum_{j=1}^{k} \sum_{i=1}^{n} P_i \, p(j/i) q_{н1}(q_{н2} + [1 - \exp(-\alpha t_{от i})](1 - q_{н2})) \qquad (7)$$

Если отдельные участки рубежа защищены по-разному, то возможны различные ситуации. Соответствующие вероятности могут быть рассчитаны аналогично.

Критерий эффективности

Для сравнения различных способов построения защиты можно применить два показателя — коэффициент сложности защиты и коэффициент безопасности. Оценки этих показателей очень субъективны и во многом зависят от опыта разработчика, хотя опыт эксплуатации систем защиты постоянно способствует их уточнению.

Показатель сложности защиты $Z = R/\delta R$ характеризует относительные затраты дополнительных ресурсов δR на защиту основных ресурсов R, причем сле-

дует учитывать затраты как на разработку и создание, так и на эксплуатацию защиты. Величина Z для разных систем колеблется в очень широких пределах. Например, при проверке полномочий пользователя в системах обработки данных Z = 0,1–0,3; в системах шифрования величина Z может составлять тысячи единиц. Проще всего коэффициент Z рассчитывается для систем охраны материальных ценностей, сложнее — для информационных систем. Тем не менее необходимо учиться оценивать ущерб от явной или неявной потери информации.

Чтобы сравнивать варианты построения системы защиты по сложности, нужно быть уверенным, что они удовлетворяют требованиям к безопасности объекта.

В общем случае вероятность нарушения безопасности объекта описывается соотношением (7), в соответствии с ним безопасность зависит от следующих факторов:

– количества типов субъектов, которые могут реализовать угрозу;

– количества типов угроз, которые могут быть реализованы на данном объекте;

– вероятности несрабатывания средств обнаружения того или иного субъекта угрозы;

– вероятности несрабатывания системы отражения той или иной угрозы;

– скорости преодоления системы защиты;

– скорости реакции системы защиты.

Все эти факторы учтены в соотношении (7) соответствующими параметрами. Если соотношение (7) используется для сравнения вариантов построения системы защиты на одном и том же объекте, то перечисленные факторы преобразуются в следующие:

– количество типов субъектов, от которых защищает данный вариант (n);

– количество рубежей защиты, которое нужно преодолеть для проникновения к s-му ресурсу (r_s) при данном варианте защиты;

– среднее время, необходимое для преодоления i-го рубежа (t_i) при реализации данного варианта защиты;

– среднее время реакции системы защиты (ликвидации угрозы) на i-м рубеже (T_i) при рассматриваемом варианте защиты.

Комплексный показатель безопасности s-го ресурса зависит от величины отношения t_i / T_i на каждом i-м рубеже защиты. Если ресурс транспортируется из одной зоны безопасности в другую, то наиболее уязвимое место там, где количество рубежей защиты минимально. Поэтому в общем случае под количеством рубежей, которое нужно преодолеть, чтобы реализовать угрозу s-му ресурсу, будем понимать минимальную величину r_s. Тогда безопасность s-го ресурса можно оценить величиной

$$W_s = \sum_{i=1}^{r_s} t_i / T_i \ ,$$

а всю систему безопасности — величиной

$$W = a_1 W_1 + a_2 W_2 + ... + a_n W_n = \sum_{s=1}^{n} a_s W_s \ ,$$

где a — весовые коэффициенты, учитывающие важность соответствующего вида ресурса. Очевидно, жизнь и здоровье людей имеют наивысший приоритет; сохранность зданий и помещений — высокий приоритет, и т.д.

Показатели Z и W имеют субъективный и приближенный характер, поэтому проектировать систему защиты, руководствуясь их абсолютными значениями, нельзя. Их следует применять только при сравнительном анализе, отбрасывая с их помощью наихудшие варианты. Для этого отметим каждый вариант точкой на плоскости Z — W (рис. 2).

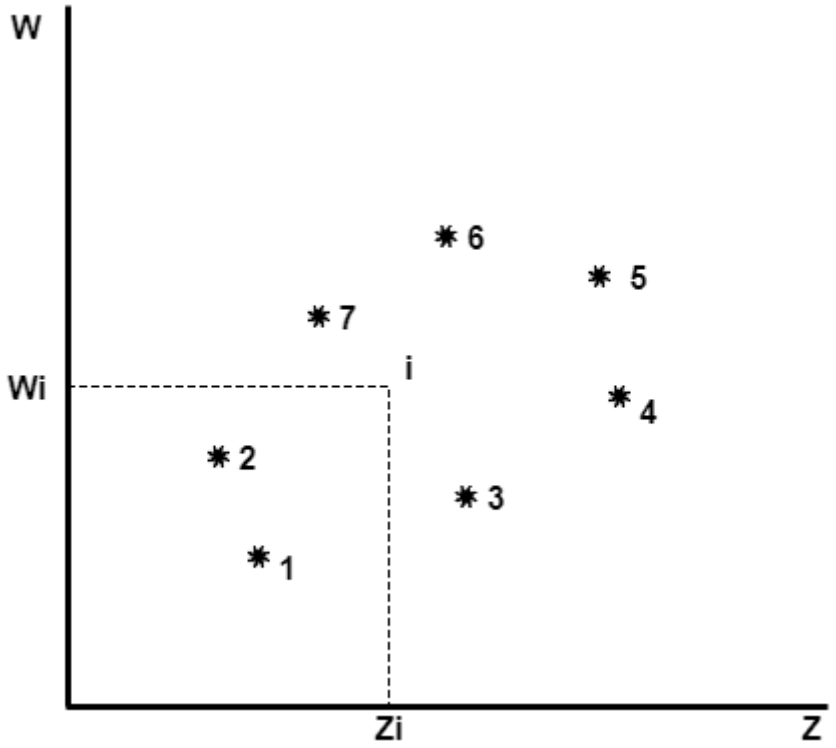


Рис. 2. Эффективность системы защиты по двум критериям — коэффициенту сложности защиты и коэффициенту безопасности

Вариант i характеризуется сложностью Z_i, и безопасностью W_i. Очевидно, что вариант 1 хуже варианта 2, так как, имея примерно равную сложность, он проигрывает ему по безопасности. То же можно сказать о вариантах 3 и 6, 4 и 5. В свою очередь, вариант 6 предпочтительнее варианта 5. Все «плохие» варианты, которые в дальнейшем не следует прорабатывать, это 1, 3, 4 и 5. Видно, что они лежат на нижней и правой границах области. Оставшиеся варианты подлежат более тщательному анализу с учетом вероятностных отношений.

Задания

1. Оценить вероятность реализации угрозы для следующих ситуаций.
Два злоумышленника на территории, количество угроз — а) 1, б) 2.
Значение величины каждой вероятности = 0,5.

Для 1-й угрозы:

$\alpha_1 = 10$;

$t_{от1} = 20$ мин;

$\alpha_2 = 30$;

$t_{от2} = 15$ мин.

Для 2-й угрозы:

$\alpha_1 = 40$;

$t_{от1} = 30$ мин;

$\alpha_2 = 60$;

$t_{от2} = 15$ мин.

Подсчет общей вероятности нарушения безопасности объекта осуществляется по формуле:

$$P = \sum_{j=1}^{k} \sum_{i=1}^{n} P_i \, p(j/i) q_{н1} (q_{н2} + [1 - \exp(-\alpha t_{отi})](1 - q_{н2})),$$

где k — число угроз; n — число нарушителей; P_i — вероятность появления субъекта i-го типа; $p(j/i)$ — условная вероятность того, что субъект i-го типа выберет для реализации угрозу j-го типа; $q_{н1}$ — вероятность несрабатывания средств обнаружения; $q_{н2}$ — вероятность несрабатывания средств отражения; α — постоянная величина, характеризующая «скорость» реализации угрозы; $t_{от}$ — время, которым располагает субъект угрозы, если $t_{от} = 0$, угроза не реализуется.

2. Привести оценки для частных случаев: A^+C^-, A^+B^+, $A^+C^+D^-$.

3. Вывести график для сравнительного анализа различных способов защиты, отмечая каждый вариант точкой на плоскости Z-W критериев эффективности.

	Вариант 1	Вариант 2	Вариант 3	Вариант 4	Вариант 5	Вариант 6
Z — сложность защиты — ось X	600	550	800	1 800	1 600	750
W — безопасность объекта — ось У	600	800	700	820	1 000	1 300

Контрольные вопросы

1. Какие угрозы относятся к естественным, а какие — к искусственным?
2. Каким путем могут осуществиться умышленные угрозы?
3. Что входит в: а) средства обнаружения; б) средства отражения; г) средства ликвидации?
4. Как можно оценить показатель сложности системы?
5. Как можно оценить безопасность s-го ресурса и всей системы безопасности?
6. Почему вариант 6 на рис. 2 предпочтительней 5, 4, 3?
7. Какие элементы входят в минимально необходимую систему защиты?

Практическая работа № 3

Исследование математических методов анализа стойкости парольных систем

Цель работы: исследование математических методов определения стойкости парольной системы.

Теоретические сведения

По статистике парольная подсистема считается самой уязвимой в современных защищенных ИС, поэтому требует самого внимательного отношения при оценке соответствия.

Пароль — идентификатор субъекта доступа, который является его (субъекта) секретом [РД «Защита от несанкционированного доступа к информации. Термины и определения» (Гостехкомиссия России, 1992)].

Согласно существующей статистике, наиболее популярными паролями пользователей являются «123456» и «qwerty». Это определяет необходимость формирования критериев стойкости парольной защиты и методов оценки выполнения установленных критериев. На сегодняшний момент существует разнообразное количество рекомендаций по выбору паролей как неофициальных подходов, так и закрепленных на законодательном уровне [РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992)].

Стойкость парольной системы оценивается для того, чтобы сделать вывод о возможности и целесообразности ее взлома (время взлома может быть настолько велико, что знание парольной информации может потерять ценность).

Основными методами взлома паролей являются:

– метод атаки по словарю (перебираются пароли, являющиеся осмысленными комбинациями символов или наиболее распространенные парольные комбинации);

– гибридные атаки (перебираются пароли из словаря, но некоторым образом дополненные). Так, гибридная атака может проверять не только пароли из словаря, но и их объединения, слова из словаря, записанные в транслитеративной форме, пароли, полученные из паролей словаря изменением символов;

– метод полного перебора (генерируются все возможные комбинации символов некоторого алфавита и подставляются в качестве паролей).

Основными объектами исследования являются пароли — комбинации определенных символов. Поскольку наибольший интерес представляет метод полного перебора (он дает гарантированный успех), то в основном задачи определения стойкости паролей сводятся к комбинаторным задачам. В связи с этим целесообразно привести основные формулы комбинаторики.

Изучение обобщенного алгоритма подбора пароля

Анализ уязвимости парольной системы требует использования ряда математических формул для определения параметров уязвимости.

Будем использовать следующие условные обозначения:

A — множество символов алфавита, используемого при переборе;

$m = |A|$ — мощность алфавита (количество символов в алфавите);

t_1 — время, затрачиваемое на генерирование одного хэш-значения в секундах;

t_2 — время сравнения двух хэш-значений в секундах;

n — число символов пароля (длина пароля в знаках);

S — мощность пространства паролей, т. е. множество всех возможных паролей в системе;

T — срок действия (жизни) пароля (обычно задается в днях).

Таким образом, число всевозможных паролей длины n, которые можно составить из символов алфавита A, составляет $S = |A|^n$.

Среди основных метрик парольной защиты могут быть выделены следующие:

– длина пароля n: большинство рекомендаций устанавливают минимальную длину пароля равной 8 символам;

– мощность алфавита пароля $|A|$: например, расширение алфавита паролей специальными символами или буквами в верхнем регистре повышает стойкость парольной системы;

– срок действия пароля T: большинство документов рекомендует использовать пароли временного действия, что позволяет повысить стойкость парольной защиты.

Пусть V — скорость подбора пароля злоумышленником, тогда вероятность подбора пароля в течение его срока действия может быть выражена следующим образом:

$$P = V \cdot T / S.$$

Обычно скорость подбора паролей и срок действия пароля можно считать известными. Задав допустимое значение вероятности подбора пароля в течение его срока действия, можно определить требуемую мощность пространства паролей S.

В общем виде алгоритм подбора пароля выглядит следующим образом:

1. Получение таблицы хэш-значений паролей.

2. Получение очередного пароля (либо из словаря, либо гибридным методом) или генерация очередной комбинации.

3. Подстановка нового пароля в алгоритм получения хэш-значения (время t_1).

4. Поочередное сравнение полученного на 3-м шаге хэш-значения с имеющимися (после п. 1) значениями в таблице (время t_2 для каждого хэш-значения таблицы). В случае совпадения данная комбинация есть действительный пароль указанного в хэш-таблице пользователя.

5. Если возможна генерация (получение) нового пароля, то осуществляется переход к п. 2.

6. Выход.

Таким образом, стойкость парольной системы определяется рядом факторов, поддающихся вполне конкретной оценке — общим числом парольных комбинаций, временем генерации хэш-значения, временем сверки хэш-значений. Для определения стойкости основным параметром выделим t — общее время полного перебора паролей. (Использование комбинаторного анализа предполагает выполнение основных принципов выбора паролей, рассмотренных на предыдущих практических занятиях).

Приведем основные производные комбинаторные формулы применительно к задаче анализа стойкости парольной системы:

Формула определения общего числа парольных комбинаций:

– если известна длина пароля n:

$$S = m^n;$$

– если известно, что длина пароля от n_1 до n_2 символов:

$$N = \sum_{i=n_1}^{n_2} m^i \ ;$$

– если известны l символов пароля и известны их места:

$$N = m^{n-l} \ .$$

Формула определения времени перебора:

$$t = N \cdot (t_1 + t_2)$$

В случае использования генераторов псевдослучайной последовательности при формировании паролей, сложность пароля можно оценить с использованием понятия энтропии. Понятие информационной энтропии было впервые формализовано Шенноном как мера неопределенности или непредсказуемости информации, неопределенность появления какого-либо символа алфавита. Энтропия множества $U = \{u_1, u_2, \ldots, u_n\}$ оценивается с использованием следующего выражения:

$$H(U) = -\sum_{t=1}^{N} p_i \cdot \log_2 p_i \ ,$$

где p_i — вероятность появления элемента u_i. Если все события появления элементов равновероятны (т. е. $p_i = 1/N$ для $\forall i \in [1, N]$, то выражение принимает вид:

$$H(U) = -\sum_{i=1}^{N} p_i \cdot \log_2 p_i = -\sum_{i=1}^{N} \frac{1}{N} \cdot \log_2 \frac{1}{N} = \log_2 N \ .$$

В случае $U = A^*$ информационная энтропия парольной системы определяется по формуле:

$$H(A^*) = \log_2 |A^*| = \log_2 |A|^n = n \cdot \log_2 |A| .$$

Величина $H(A^*)$ характеризует степень случайности пароля при его генерации и показывает, насколько сложно его угадать злоумышленнику. Например, для известного пароля энтропия равна нулю. Если пароль имеет энтропию равную 1 символу, то угадать его с первой попытки можно с вероятностью равной $1/|A|$.

Задания

1. Определить время подбора 5 паролей, если известно, что длина каждого из них не превосходит n_2 символов, пароли набираются на алфавитно-цифровой клавиатуре (без использования «Shift») (учесть возможность сверки всех 5 паролей для одного хэш-значения) (параметры n_2, t_1, t_2 см. в табл. 1).

Таблица 1

Вариант	Задание							
	1			2	3	4		
	n_2	t_1	t_2	m	n	n_2	t_1	t_2
1	10	$1{,}0\cdot10^{-6}$	$5{,}4\cdot10^{-7}$	36	6	7	$2{,}8\cdot10^{-6}$	$1{,}2\cdot10^{-7}$
2	9	$2{,}5\cdot10^{-6}$	$7{,}3\cdot10^{-7}$	38	13	8	$7{,}2\cdot10^{-6}$	$8{,}9\cdot10^{-7}$
3	8	$2{,}2\cdot10^{-6}$	$8{,}3\cdot10^{-7}$	30	8	9	$6{,}0\cdot10^{-6}$	$8{,}2\cdot10^{-7}$
4	7	$1{,}3\cdot10^{-6}$	$9{,}7\cdot10^{-7}$	53	7	10	$2{,}8\cdot10^{-6}$	$4{,}6\cdot10^{-7}$
5	9	$1{,}3\cdot10^{-6}$	$5{,}3\cdot10^{-7}$	51	6	8	$2{,}5\cdot10^{-6}$	$2{,}2\cdot10^{-7}$
6	8	$2, \cdot10^{-6}$	$4{,}4\cdot10^{-7}$	46	12	8	$8{,}2\cdot10^{-6}$	$5{,}6\cdot10^{-7}$
7	9	$5{,}9\cdot10^{-6}$	$3{,}2\cdot10^{-7}$	39	13	9	$2{,}2\cdot10^{-6}$	$6{,}6\cdot10^{-7}$
8	8	$1{,}6\cdot10^{-6}$	$8{,}2\cdot10^{-7}$	32	13	9	$3{,}3\cdot10^{-6}$	$2{,}7\cdot10^{-7}$
9	7	$2{,}8\cdot10^{-6}$	$4{,}5\cdot10^{-7}$	42	7	10	$2{,}9\cdot10^{-6}$	$6{,}6\cdot10^{-7}$
10	10	$7{,}0\cdot10^{-6}$	$8{,}2\cdot10^{-7}$	53	12	6	$1{,}8\cdot10^{-6}$	$2{,}1\cdot10^{-7}$
11	9	$1{,}6\cdot10^{-6}$	$7{,}3\cdot10^{-7}$	42	11	5	$5{,}1\cdot10^{-6}$	$1{,}0\cdot10^{-7}$
12	8	$1{,}7\cdot10^{-6}$	$2{,}3\cdot10^{-7}$	37	7	8	$1{,}3\cdot10^{-6}$	$3{,}3\cdot10^{-7}$
13	6	$2{,}1\cdot10^{-6}$	$8{,}1\cdot10^{-7}$	53	8	8	$6{,}0\cdot10^{-6}$	$8{,}4\cdot10^{-7}$
14	7	$1{,}9\cdot10^{-6}$	$1{,}1\cdot10^{-7}$	38	12	9	$1{,}5\cdot10^{-6}$	$3{,}6\cdot10^{-7}$
15	7	$1{,}1\cdot10^{-6}$	$3{,}7\cdot10^{-7}$	37	7	6	$9{,}0\cdot10^{-6}$	$7{,}0\cdot10^{-7}$

2. Найти минимальную длину пароля n, при которой пароль не будет взломан в течение 1 года (при постоянном переборе) при количестве символов алфавита m, и скорости перебора 500 000 пар/сек. (параметр m см. в табл. 1).

3. Определить минимальную мощность множества символов алфавита m, при котором пароль длиной n не будет взломан в течение 3 мес. при скорости перебора 500 000 пар/сек. (параметр n см. в табл. 1).

4. Определить время подбора пароля, если известно, что его длина не превосходит n_2 символов, пароль набираются на алфавитно-цифровой клавиатуре (с использованием Shift), а также известно, что в пароле точно есть символы «m», «k», «p» (параметры n_2, t_1, t_2 см. в табл. 1).

5. Определить формулу для расчета общего числа парольных комбинаций, если известно, что в пароле от n_1 до n_2 символов, а также известно, что из m символов алфавита $M=\{M_1, M_2, ..., M_m\}$ символы $\{M_1, M_2, ..., M_k\}$ встречаются в пароле точно, а символы $\{M_{k+1}, M_{k+2}, ..., M_{k+r}\}$ не встречаются точно.

6. Рассчитать минимальный срок действия пароля T дней длиной n символов, при котором обеспечивается требуемый уровень надежности парольной защиты (вероятность вскрытия 10^{-4}). Пароли набираются на алфавитно-цифровой клавиатуре (без использования «Shift») при возможности получения хэш-значения за время t_1 и сравнения полученного хэш-значения с имеющимися значениями в таблице за время t_2 (параметры n, t_1, t_2 см. в табл. 2).

7. Определить значение энтропии для заданных алфавитов A и паролей длины n, а также суммарную энтропию для паролей длины от 1 символа до n (значения A и n по вариантам см. в табл. 2).

Таблица 2

Вариант	Задание 6			Задание 7	
	n	t_1	t_2	A	n
1	10	$2{,}8\cdot10^{-6}$	$1{,}2\cdot10^{-7}$	Арабские цифры (0–9), 10 символов	10
2	12	$7{,}2\cdot10^{-6}$	$8{,}9\cdot10^{-7}$	Шестнадцатеричные числа (0–9, A–F), 16 символов	12
3	7	$6{,}0\cdot10^{-6}$	$8{,}2\cdot10^{-7}$	Латинский алфавит (a–z, A–Z), 52 символа	7
4	11	$2{,}8\cdot10^{-6}$	$4{,}6\cdot10^{-7}$	Латинский алфавит с цифрами (a–z, A–Z, 0–9), 62 символа	11
5	6	$2{,}5\cdot10^{-6}$	$2{,}2\cdot10^{-7}$	Таблица ASCII, 94 символа	6
6	10	$8{,}2\cdot10^{-6}$	$5{,}6\cdot10^{-7}$	Арабские цифры (0–9), 10 символов	10
7	13	$2{,}2\cdot10^{-6}$	$6{,}6\cdot10^{-7}$	Шестнадцатеричные числа (0–9, A–F), 16 символов	13
8	13	$3{,}3\cdot10^{-6}$	$2{,}7\cdot10^{-7}$	Латинский алфавит (a–z, A–Z), 52 символа	13
9	8	$2{,}9\cdot10^{-6}$	$6{,}6\cdot10^{-7}$	Латинский алфавит с цифрами (a–z, A–Z, 0–9), 62 символа	8
10	11	$1{,}8\cdot10^{-6}$	$2{,}1\cdot10^{-7}$	Таблица ASCII, 94 символа	11
11	12	$5{,}1\cdot10^{-6}$	$1{,}0\cdot10^{-7}$	Арабские цифры (0–9), 10 символов	12
12	11	$1{,}3\cdot10^{-6}$	$3{,}3\cdot10^{-7}$	Шестнадцатеричные числа (0–9, A–F), 16 символов	11
13	7	$6{,}0\cdot10^{-6}$	$8{,}4\cdot10^{-7}$	Латинский алфавит (a–z, A–Z), 52 символа	7
14	8	$1{,}5\cdot10^{-6}$	$3{,}6\cdot10^{-7}$	Латинский алфавит с цифрами (a–z, A–Z, 0–9), 62 символа	8
15	12	$9{,}0\cdot10^{-6}$	$7{,}0\cdot10^{-7}$	Таблица ASCII, 94 символа	12

Контрольные вопросы

1. С какой целью производится анализ стойкости парольной системы?
2. Какие методы используются при анализе стойкости парольной системы?
3. Какие комбинаторные объекты используются при полном переборе?
4. Какие параметры стойкости можно считать приемлемыми?
5. Опишите и поясните основные шаги обобщенного алгоритма подбора паролей.

Практическая работа № 4

Управление доступом. Домены безопасности. Модель распространения прав доступа

Цель работы: познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере дискреционной модели.

Теоретические сведения

Дискреционная политика безопасности

Существуют два типа политики безопасности: дискреционная и мандатная. В данной практической работе рассматривается первый вид политики безопасности.

Основой дискреционной (дискретной) политики безопасности является дискреционное управление доступом (Discretionary Access Control — DAC), которое определяется двумя свойствами:

– все субъекты и объекты должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

Термин «дискреционная политика» является дословным переводом Discretionary policy, еще одним вариантом перевода является следующий — разграничительная политика. Рассматриваемая политика — одна из самых распространенных в мире, в системах по умолчанию имеется ввиду именно эта политика.

Пусть O — множество объектов, S — множество субъектов, $S \subseteq O$. Пусть $U=\{U_1, ..., U_m\}$ — множество пользователей. Определим отображение: own: $O \rightarrow U$.

В соответствии с этим отображением каждый объект объявляется собственностью соответствующего пользователя. Пользователь, являющийся собственником объекта, имеет все права доступа к нему, а иногда и право передавать часть или все права другим пользователям. Кроме того, собственник объекта определяет права доступа других субъектов к этому объекту, то есть политику безопасности в отношении этого объекта. Указанные права доступа записываются в виде матрицы доступа, элементы которой — суть подмножества множества R, определяющие доступы субъекта S, к объекту O_i (i = 1, 2, ...; j = 1, 2, ...).

	O_1	O_2	…	O_k	S_1	…	S_n
S_1	own R	W	…				
S_2							
⋮							
S_n							

Существует несколько вариантов задания матрицы доступа.

1. **Списки полномочий субъектов (списки возможностей)**: Для каждого субъекта S_i создается список (файл) всех объектов, к которому имеет доступ данный объект.

2. **Списки управления доступом (Access — ACT Control List)**: для каждого объекта создается список всех субъектов, имеющих право доступа к этому объекту.

Дискреционная политика связана с исходной моделью таким образом, что траектории процессов в вычислительной системе ограничиваются в каждом доступе. Причем вершины каждого графа разбиваются на классы и доступ в каждом классе определяется своими правилами каждым собственником. Множество неблагоприятных траекторий N для рассматриваемого класса политик определяется наличием неблагоприятных состояний, которые в свою очередь определяются запретами на некоторые дуги. Дискреционная политика, как самая распространенная, больше всего подвергалась исследованиям. Существует множество разновидностей этой политики. Однако многих проблем защиты эта политика решить не может. Одна из самых существенных слабостей этого j класса политик — то, что они не выдерживают атак при помощи «Троянского коня». Это означает, в частности, что система защиты, реализующая дискреционную политику, плохо защищает от проникновения вирусов в систему и других средств скрытого разрушающего воздействия. Покажем на примере принцип атаки «Троянским конем» в случае дискреционной политики.

Пример 1. Пусть U_1 — некоторый пользователь, а U_2 — пользователь-злоумышленник, O_1 — объект, содержащий ценную информацию, O_2 — программа с «Троянским конем» T, и M — матрица доступа, которая имеет вид:

	O_1	O_2
U_1	Own R W	W
U_2		Own R W

Проникновение программы происходит следующим образом. Злоумышленник U_2 создает программу O_2 и, являясь ее собственником, дает U_1 запускать ее и писать в объект O_2 информацию. После этого он инициирует каким-то образом, чтобы U_1 запустил эту программу (например, O_2 — представляет интересную компьютерную игру, которую он предлагает U_1 для развлечения). U_1 запускает O_2 и тем самым запускает скрытую программу T, которая обладая правами U_1 (так как была запущена пользователем U_1), списывает в себя информацию, содержащуюся в O_1. После этого хозяин U_2 объекта O_2, пользуясь всеми правами, имеет возможность считать из O_2 ценную информацию объекта O_1.

Следующая проблема дискреционной политики — это автоматическое определение прав. Так как объектов много, то задать заранее вручную перечень

прав каждого субъекта на доступ к объекту невозможно. Поэтому матрица доступа различными способами агрегируется, например, оставляются в качестве субъектов только пользователи, а в соответствующую ячейку матрицы вставляются формулы функций, вычисление которых определяет права доступа субъекта, порожденного пользователем, к объекту *O*. Разумеется, эти функции могут изменяться во времени. В частности, возможно изъятие прав после выполнения некоторого события. Возможны модификации, зависящие от других параметров.

Одна из важнейших проблем при использовании дискреционной политики — это проблема контроля распространения прав доступа. Чаще всего бывает, что владелец файла передает содержание файла другому пользователю и тот, тем самым, приобретает права собственника на информацию. Таким образом, права могут распространяться, и даже, если исходный владелец не хотел передавать доступ некоторому субъекту S к своей информации в O, то после нескольких шагов передача прав может состояться независимо от его воли. Возникает задача об условиях, при которых в такой системе некоторый субъект рано или поздно получит требуемый ему доступ.

К достоинствам дискреционной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. Этим обусловлен тот факт, что большинство распространенных в настоящее время ИС обеспечивают выполнение положений именно данной политики безопасности.

В качестве примера реализаций дискреционной политики безопасности в ИС можно привести матрицу доступов, строки которой соответствуют субъектам системы, а столбцы — объектам; элементы матрицы характеризуют права доступа. К недостаткам относится статичность модели. Это означает, что данная политика безопасности не учитывает динамику изменений состояния ИС, не накладывает ограничений на состояния системы.

Кроме этого, при использовании дискреционной политики безопасности возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность ИС. В общем случае при использовании данной политики безопасности стоит алгоритмически неразрешимая задача: проверить приведут ли его действия к нарушению безопасности или нет. В то же время имеются модели ИС, реализующих дискреционную политику безопасности (например, модель Take-Grant), которые предоставляют алгоритмы проверки безопасности.

Так или иначе, матрица доступов не является тем механизмом, который бы позволил реализовать ясную и четкую систему защиты информации в ИС. Этим обуславливается поиск других более совершенных политик безопасности.

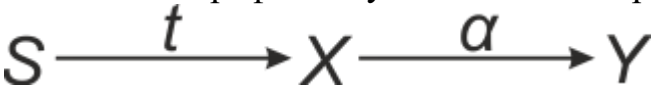
Модель распространения прав доступа Take-Grant

Модель распространения прав доступа Take-Grant используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. В качестве основных элементов модели используются граф доступов и правила его преобразования. Цель модели — дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов.

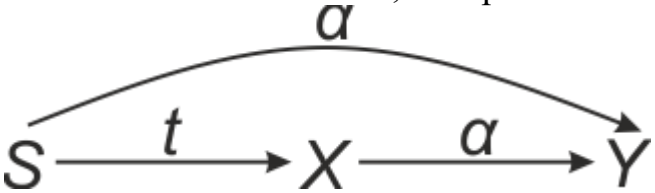
В модели Take-Grant строится граф доступов субъектов к объектам и используются права доступа $R=\{r, w, c\}$, где r — читать, w — писать, c — исполнять. Допускается, что субъект X может иметь права $\alpha \subseteq R$ на доступ к объекту Y, эти права записываются в матрице контроля доступов. Кроме этих прав модель предусматривает еще два: право take (t) — **брать права доступа** и право grant (g) — **передавать права доступа**, которые также записываются в матрицу контроля доступов субъекта к объектам.

Эти права определяют возможности преобразования одних графов состояний в другие. Преобразование состояний, то есть преобразование графов доступов, проводятся при помощи команд. Существует четыре вида команд, по которым один граф доступа преобразуется в другой.

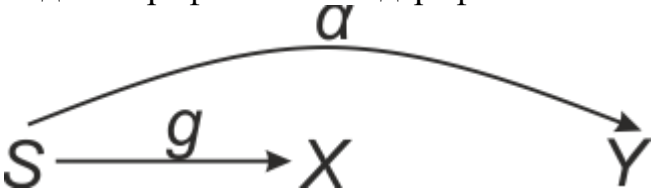
1. **Take**. Пусть S — субъект, обладающий правом t к объекту X и $\alpha \subseteq R$ некоторое право доступа объекта X к объекту Y. Тогда возможна команда «S take α for Y from X». В результате выполнения этой команды в множество прав доступа субъекта S к объекту Y добавляется право α. Графически это означает, что, если в исходном графе доступов G был подграф



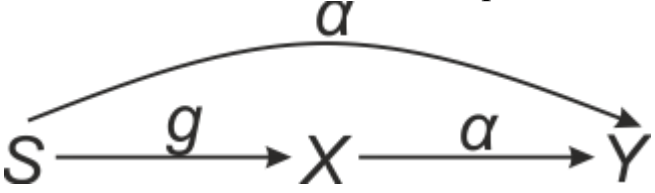
то в новом состоянии G', построенном по этой команде t, будет подграф



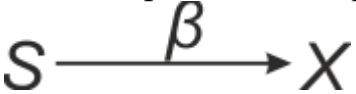
2. **Grant**. Пусть субъект S обладает правом g к объекту X и правом $\alpha \subseteq R$ к объекту Y. Тогда возможна команда «S grant α for Y to X». В результате выполнения этой команды граф доступов G преобразуется в новый граф G', который отличается от G добавленной дугой (X Y). Графически это означает, что если в исходном графе G был подграф



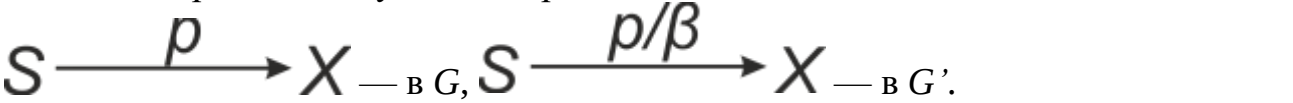
то в новом состоянии G', построенном по команде g, будет подграф



3. **Create**. Пусть S — субъект, $\beta \subseteq R$. Команда «S create β for new object X» создает в графе новую вершину X и определяет β как права доступов S к X. То есть по сравнению с графом G в новом состоянии G' добавляется подграф вида



4. **Remove**. Пусть S — субъект и X — объект, $\beta \subseteq R$. Команда «S remove β for X» исключает права доступа β из прав субъекта S к объекту X. Графически преобразования графа доступа G в новое состояние G' в результате этой команды можно изобразить следующим образом:



Под безопасностью понимается возможность или невозможность произвольной фиксированной вершине P получить доступ $\alpha \in R$ к произвольной фиксированной вершине X путем преобразования текущего графа G некоторой последовательностью команд в граф G', где указанный доступ разрешен.

Домены безопасности

В рамках рассматриваемой модели ИС как совокупности субъектов и объектов разграничение доступа субъектов к объектам может быть реализовано на основе таблицы, содержащей разрешенные типы доступа и называемой матрицей доступа. Как правило, матрица доступа (табл. 3) имеет большие размеры (в системе присутствует множество различных субъектов и объектов) и является разреженной (субъектам необходим доступ только к небольшим подмножествам объектов).

Таблица 3

		Объекты			
		1	2	…	m
Субъекты	1	Чтение	Чтение		Исполнение
	2	Чтение	Чтение/Запись		Чтение/запись
	…				
	n	Запись	Исполнение		Нет доступа

Под доменом безопасности понимается совокупность объектов, к которым разрешен доступ конкретному субъекту.

В табл. 3 домены безопасности представлены отдельными строками. В соответствии с обсуждаемым ниже принципом минимизации привилегий домен безопасности данного субъекта должен включать минимально возможный набор объектов и связанных с ними прав доступа, необходимый для работы субъекта. Тем самым снижается риск злоупотребления правами доступа со стороны субъекта и уменьшается разрушительный эффект от потенциального злоупотребления. Для реализации этого принципа необходимо, чтобы субъекты, которым необходимо выполнять множество различных операций, могли поочередно работать в нескольких небольших (в смысле числа составляющих их объектов и назначенных прав доступа к этим объектам) доменах, переключаемых при необходимости. Следующие факторы определяют минимально возможные по практическим соображениям размеры доменов:

- гибкость и простота механизма переключения доменов;
- размер защищаемых объектов;
- наличие разных способов изменения матрицы доступа;

– гибкость в определении произвольных типов доступа к объектам.

В ИС переключение доменов безопасности может происходить, в частности, при вызове из основной программы некоторой процедуры или функции, или, говоря в терминах рассмотренной выше субъектно-объектной модели, в момент порождения одним субъектом (выполняющейся программы) нового субъекта (вызываемой процедуры) из некоторого объекта (области памяти, содержащей код процедуры). По завершении выполнения вызванной процедуры происходит обратное переключение домена безопасности.

Если с вызовом процедуры связано переключение доменов безопасности, процедура называется защищенной. Такая процедура фигурирует в матрице доступа и в качестве субъекта, и в качестве объекта. Первое объясняется тем, что процедура функционирует в собственном домене безопасности. Второе — тем, что по отношению к данной процедуре могут быть назначены права доступа, в частности право «исполнить».

Рассмотрим пример, где права доступа заданы согласно табл. 4.

Таблица 4

		Объекты		
		Файл программы редактора текстов	Текстовый файл	Словарь
Субъекты	…			
	Пользователь	Исполнить	Чтение/Запись	
	Программа редактор		Чтение/Запись	Чтение
	…			

Пользователь имеет доступ к текстовому файлу как при помощи текстового редактора, так и из собственного домена безопасности. Однако доступ к словарю для пользователя становится возможен только при переключении на домен безопасности редактора (путем запуска на исполнение программы редактора). При таком способе переключения доменов матрица доступа после переключения остается неизменной.

Более сложный случай переключения доменов связан с передачей прав доступа в качестве параметров вызываемой процедуре и сопровождается изменением матрицы доступа. Предположим, что права доступа заданы так, как показано в табл. 5.

В отличие от предыдущего случая, редактор не имеет права доступа к текстовому файлу пользователя. При вызове редактора это право должно быть ему передано, и в матрице доступа будет создана новая, временная строка (табл. 6).

Таблица 5

		Объекты		
		Файл программы редактора текстов	Текстовый файл	Словарь
Субъекты	…			
	Пользователь	Исполнить	Чтение/Запись	
	Программа редактор			Чтение
	…			

Таблица 6

		Объекты		
		Файл программы редактора текстов	Текстовый файл	Словарь
Субъекты	…			
	Пользователь	Исполнить	Чтение/Запись	
	Программа редактор			Чтение
	Редактор, действующий от имени пользователя		Чтение/Запись	Чтение
	…			

Созданный при этом временный домен безопасности описывает стандартное право текстового редактора на доступ к словарю и переданное ему при вызове право на доступ к файлу пользователя. Этот домен безопасности уничтожается по завершению работы редактора.

В рассмотренных примерах переключение доменов безопасности было связано либо только с потерей прав (например, пользователь теряет доступ к словарю, завершив работу с редактором), либо только с их приобретением (редактор при запуске получает доступ к текстовому файлу). Данная концепция доменов безопасности может быть расширена и на случай, когда потеря и приобретение различных прав доступа одним субъектом происходят при переключении домена безопасности одновременно, а также на случай, когда вызываемые процедуры являются реентерабельными.

Задания

Дискреционная политика безопасности

Исследуемая система состоит из множества субъектов и объектов.

Исходные данные:

СУБЪЕКТЫ

1. Пользователь1 (Администратор).
2. Пользователь 2.
3. Пользователь 3.
4. Текстовый редактор Word.
5. Редактор формул.
6. Модуль проверки правописания.

ОБЪЕКТЫ

1. Документ пользователя 1.
2. Документ пользователя 2.
3. Документ пользователя 3.
4. Файл текстового редактора Word WINWORD.EXE.
5. Файл редактора формул EQUATION.DLL.
6. Файл модуля проверки правописания SPELL.DLL.
7. Файл-словарь DICTIONARY.DOC.

Политика безопасности системы устанавливает такой порядок работы, при котором:

– пользователь 1 имеет возможность работы со своим документом с помощью программы WORD, может только просматривать документы пользователя 2 и 3, может проверять правописание в своем документе и вставлять в него формулы; также пользователь1 может добавлять новые слова в словарь;

– пользователь 2 имеет возможность работать только со своим документом, может проверять правописание, но не может добавлять новые слова в словарь и не может вставлять в документ формулы;

– пользователь 3 имеет возможность работать со своим документов и документом пользователя 2, может проверять правописание в обоих документах, может добавлять в документы формулы, но не может добавлять новые слова в словарь.

Программа Word может быть запущена только пользователями системы, и может вызывать редактор формул и модуль проверки правописания.

Только модуль проверки правописания может изменять файл-словарь DICTIONARY.DOC.

Необходимо

1. Составить множество возможных прав доступа в системе. Для заданного множества субъектов и объектов построить матрицу доступа и заполнить ее в соответствии заданной политикой безопасности и с принципом минимизации привилегий.

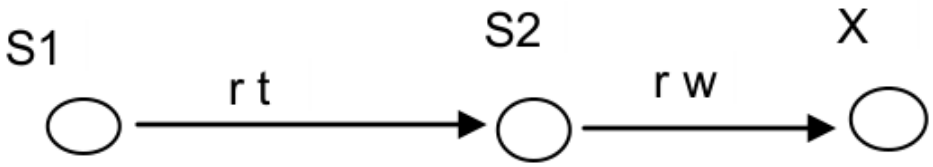
2. Дополнить матрицу доступа временными доменами (например, добавить строку «Программа Word, запущенная от имени первого пользователя или «Редактор формул, запущенный третьим пользователем из программы Word»). В матрице доступа должны быть представлены временные домены для всех возможных комбинаций взаимодействующих субъектов.

Модель Take-Grant

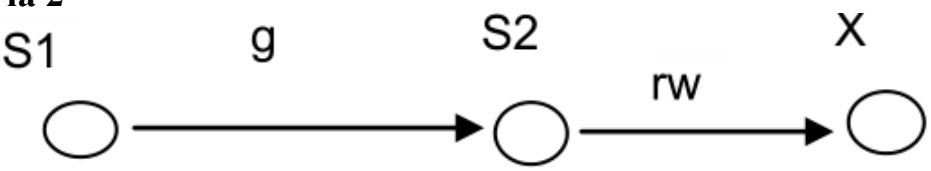
1. Для заданной задачи показать последовательность команд, которая позволяет субъекту S1 в санкционированном режиме получить право r на объект X. В базовой модели используется 4 команды преобразования графа доступов:

1. *S* take *a* for *Y* from *X* (субъект *S* берет у объекта *X* права *a* на объект *Y*).
2. *S* grant *a* for *Y* to *X* (субъект *S* дает объекту *X* права *a* на объект *Y*).
3. *S* create *a* for new object *X* (субъект *S* создает новый *a*-доступный объект *X*).
4. *S* remove *a* for *X* (субъект *S* удаляет права доступа *a* на объект *X*).

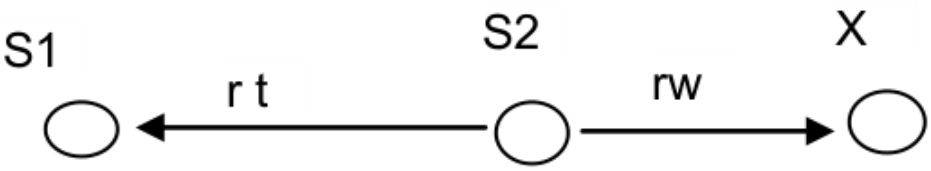
Задача 1



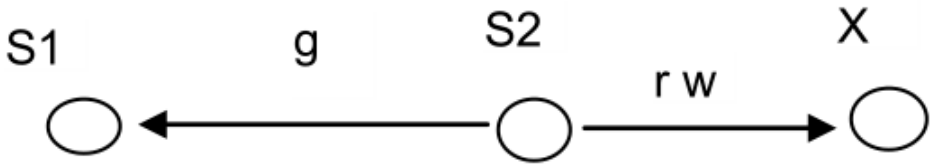
Задача 2



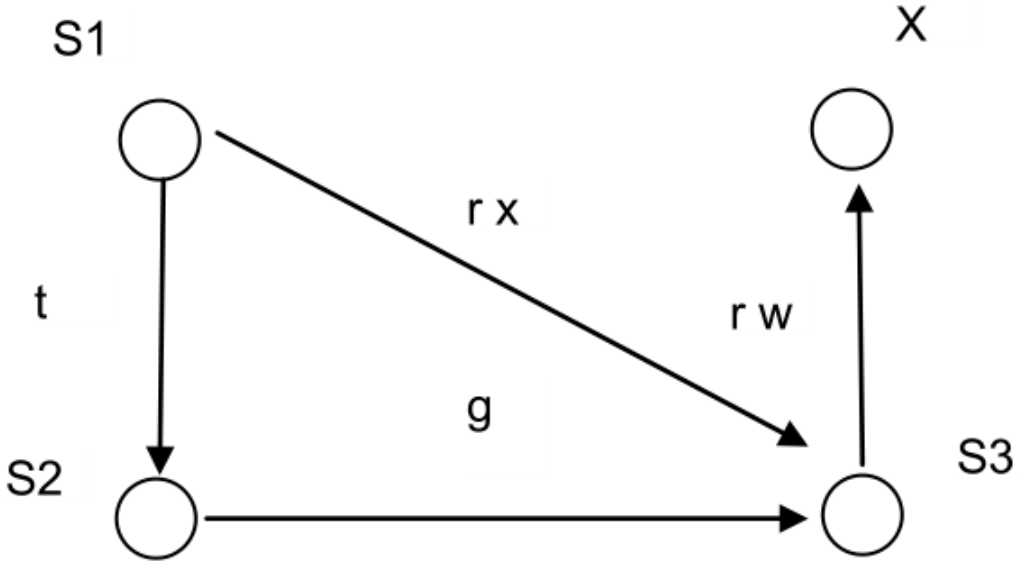
Задача 3



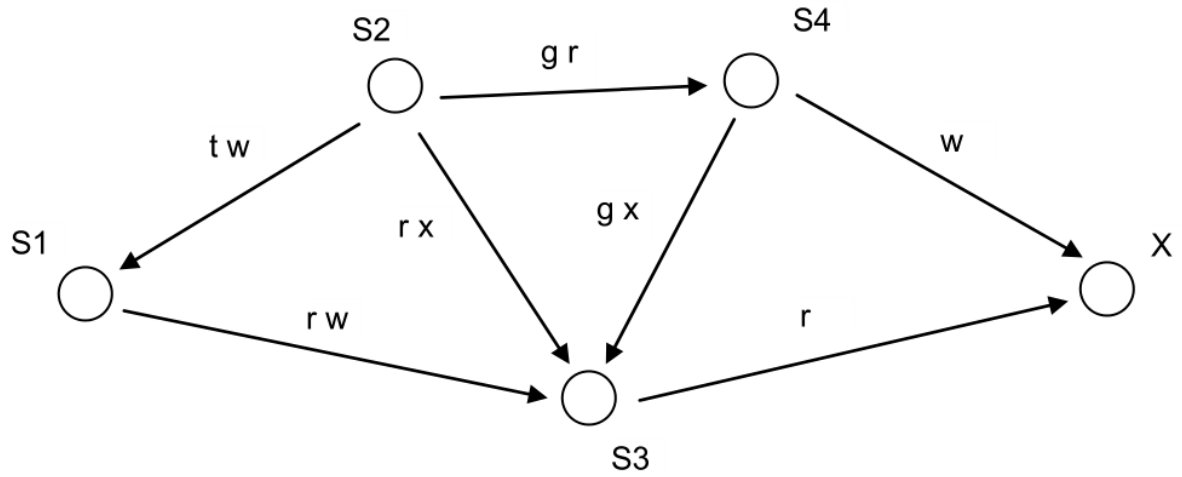
Задача 4



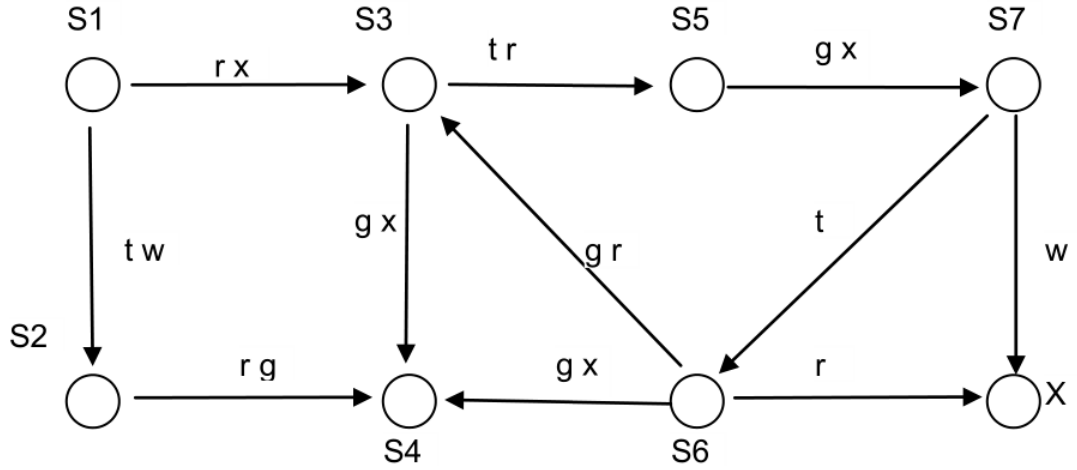
Задача 5



Задача 6



2. Для заданного графа доступов показать, что субъект S1 может похитить право r на объект X.



Контрольные вопросы

1. Дайте определение дискреционной политики безопасности.
2. Дайте определение доменов безопасности, применим ли механизм доменов безопасности в системах с мандатным разграничением доступа.
3. В каких случаях в матрицу доступа добавляется временный домен безопасности.
4. Какие существуют правила при формировании прав доступа во временном домене.
5. Каково назначение модели Take-Grant, для каких систем применима данная модель.
6. Каково назначение прав доступа take и grant, какие возможности предоставляются субъекту, обладающему такими правами.

Практическая работа № 5

Управление доступом. Реализация мандатной модели политики безопасности

Цель работы: познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере мандатной модели.

Теоретические сведения

Основу мандатной (полномочной) политики безопасности составляет мандатное управление доступом (Mandatory Access Control — MAC), которое подразумевает, что:

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– задан линейно упорядоченный набор меток секретности;

– каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации — его уровень секретности в ИС;

– каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в ИС — максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа.

Основная цель мандатной политики безопасности — предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т. е. противодействие возникновению в ИС информационных каналов сверху вниз.

Чаще всего мандатную политику безопасности описывают в терминах, понятиях и определениях свойств модели Белла-ЛаПадула. В рамках данной модели доказывается важное утверждение, указывающее на принципиальное отличие систем, реализующих мандатную защиту, от систем с дискреционной защитой: если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.

Кроме того, по сравнению с ИС, построенными на основе дискреционной политики безопасности, для систем, реализующих мандатную политику, характерна более высокая степень надежности. Это связано с тем, что монитор безопасности такой системы должен отслеживать, не только правила доступа субъектов системы к объектам, но и состояния самой ИС. Таким образом, каналы утечки в системах данного типа не заложены в нее непосредственно (что мы наблюдаем в положениях предыдущей политики безопасности), а могут появиться только при практической реализации системы вследствие ошибок разработчика. В дополнении к этому правила мандатной политики безопасности более ясны и просты для понимания разработчиками и пользователями ИС, что также является фактором, положительно влияющим на уровень безопасности системы. С другой стороны,

реализация систем с политикой безопасности данного типа довольно сложна и требует значительных ресурсов вычислительной системы.

Мандатный принцип разграничения доступа ставил своей целью перенести на автоматизированные системы практику секретного документооборота, принятую в правительственных и военных структурах, когда все документы и допущенные к ним лица ассоциируются с иерархическими уровнями секретности. Критерием безопасности является невозможность получения информации из документов определенного уровня безопасности работником, чей уровень безопасности, т. е. уровень доверия, ниже, чем уровень безопасности соответствующих документов.

Данный критерий безопасности фактически означает запрет определенных информационных потоков, которые трактуются как опасные и недопустимые.

Кроме того, были проанализированы правила и система назначений, изменений, лишений и т. д. допусков сотрудников к работе с секретными документами, правила создания, уничтожения документов, присвоения или изменения грифов их секретности, в том числе и рассекречивания, а также другие особенности работы с секретными документами. В частности, было отмечено, что правила получения доступа к документам различаются в зависимости от характера работы с ними — изучение (чтение) или изменение (создание, уничтожение, внесение дополнений, редактирование, т. е. запись в них). На этой основе было «выявлено» два основных правила, гарантирующих безопасность:

Правило 1. **No read up** (NRU — нет чтения вверх). Работник не имеет права знакомиться с документом (читать), гриф секретности (уровень безопасности) которого выше его степени допуска (уровня безопасности).

Правило 2. **No write down** (NWD — нет записи вниз). Работник не имеет права вносить информацию (писать) своего уровня безопасности в документ с более низким уровнем безопасности (с более низким грифом секретности).

Первое правило является естественным и очевидным способом обеспечения безопасности при осуществлении информационных потоков из документов к работникам и иначе может быть сформулировано так: работнику нельзя получать информацию, уровень секретности которой выше его уровня доверия. Второе правило обеспечивает безопасность при осуществлении информационных потоков от работника к документу и иначе может быть сформулировано так: работнику нельзя передавать информацию своего уровня секретности в тех случаях, когда в результате передачи с ней могут ознакомиться работники с более низким уровнем безопасности.

При представлении работников, работающих с секретными документами, субъектами доступа, а секретных документов в качестве объектов доступа ИС, буквальное следование правилу NWD приводит к автоматическому включению в механизмы обеспечения безопасности субъективного фактора в лице субъекта-пользователя, который при внесении информации в объекты-документы с более низким грифом секретности должен субъективно оценить соответствие вносимой информации уровню безопасности документа. Задача исключения данного субъективного фактора может решаться различными способами, самым простым

из которых является полный запрет изменения субъектами (доступ write) объектов с уровнем безопасности, более низким, чем уровень безопасности соответствующих субъектов.

Задания

1. Пусть имеется мандатная система доступа, в которой решетка уровней безопасности является линейной и имеет три уровня — l_1, l_2, l_3; $l_1 > l_2 > l_3$; $l_1 > l_3$.

Пусть имеется следующая система субъектов (пользователей) доступа:

*s*1 — администратор системы;

*s*2 — руководитель предприятия;

*s*3 — делопроизводитель;

*s*4 — user, т. е. рядовой непривилегированный пользователь.

Пусть имеется следующая система объектов доступа:

*o*1 — системное ПО;

*o*2 — документ «Стратегия выхода предприятия на новые рынки сбыта продукции»;

*o*3 — документ «Приказ о поощрении работников по случаю Дня предприятия»;

*o*4 — АИС — прием, обработка и исполнение заказов клиентов (ПО и БД).

1.1. Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа A[*s*, *o*].

2. Заданы документы с различным уровнем секретности, заданы пользователи с различным уровнем доступа (список документов и пользователей и их уровни доступа/секретности составить самостоятельно. Не менее 5 пользователей и 5 документов).

2.1. Для каждого пользователя составить список документов, доступных ему для работы при условии, что пользователь не понижает своего уровня допуска.

2.2. Для одного из пользователей определить права доступа к документам при условии, что пользователь может понизить свой уровень доступа на один уровень.

2.3. Один из пользователей имеет возможность работать с несколькими документами. На основе этих документов он создает новый документ. Какой гриф секретности нужно присвоить этому документу.

2.4. Показать на примере одного из пользователей, что мандатная политика безопасности не может быть нарушено программой типа «Троянский конь».

3. Заданы субъекты и объекты с различными уровнями допуска/секретности. Задана матрица доступов для первоначального состояния системы A[*s*, *o*] (см. ниже).

3.1. Показать, что первоначальное состояние A[*s*, *o*] является безопасным состоянием — т. е. удовлетворяет свойствам безопасности:

– запрет чтения информации субъектом с уровнем безопасности меньшим, чем у объекта, из которого информация читается (NO READ UP, «не читать выше» — NRU);

– запрет записи информации субъектом с уровнем безопасности большим, чем у объекта, в который информация записывается (NO WRITE DOWN, «не записывать ниже» — NWD).

При условии, что осуществляются только доступы, описанные в матрице доступов.

3.2. Если условия безопасности не выполняются, то показать пути изменения исходного задания (понижение уровня доступа пользователей или изменение матрицы доступов), которые позволят выполнить условия безопасности). Понижать уровень секретности документов нельзя.

S={*s*1, *s*2, *s*3, *s*4, *s*5}.

O={*o*1, *o*2, *o*3, *o*4, *o*5}.

L={1 — низкий, 2 — средний, 3 — высокий, 4 — максимальный}.

Таблица 7

Максимальный уровень доступа субъектов

S	*s*1	*s*2	*s*3	*s*4	*s*5
fs	1	4	3	2	3

Таблица 8

Уровень секретности объектов

O	*o*1	*o*2	*o*3	*o*4	*o*5
fo	1	3	2	4	4

Таблица 9

Матрица доступов

M	*o*1	*o*2	*o*3	*o*4	*o*5
*s*1	*re*				
*s*2		*r*	*e*		
*s*3		*rw*	*w*	*we*	
*s*4				*rwe*	
*s*5					*rwe*

Контрольные вопросы

1. Дайте определение мандатного управления доступом.

2. Объясните, почему системы, реализующие мандатное управление доступом устойчивы к атакам с помощью программ типа «Троянский конь».

3. Перечислите и поясните свойства, которыми должна обладать безопасная система согласно модели Белла-ЛаПадула.

4. В чем заключается модель мандатной политики безопасности в компьютерной системе?

5. Перечислить группу аксиом, определяющих мандатную модель политики безопасности.

6. Какой уровень допуска должен иметь администратор компьютерной системы?

Практическая работа № 6

Модель ролевого доступа при иерархически организованной системе ролей

Цель работы: познакомиться с концепцией ролевого управления доступом.

Теоретические сведения

В основе рассмотренных ранее политик безопасности лежат отношения между отдельным пользователем (субъектом) и объектом доступа, определяемые либо внешним фактором (дискреционный доступ), либо уровнем безопасности (мандатный доступ).

Вместе с тем, анализ различных организационно-управленческих и организационно-технологических схем, показывает, что в реальной жизни сотрудники предприятий, учреждений выполняют определенные функциональные обязанности не от своего личного имени, а в рамках некоторой должности. Должность, которую можно трактовать как определенную роль, представляет некоторую абстрактную, точнее обобщенную сущность, выражающую определенный тип функций и тип положения работника (подчиненность, права и полномочия). Таким образом, в реальной жизни в большинстве организационно-технологических схем права и полномочия предоставляются конкретному сотруднику не лично (непосредственно), а через назначение его на определенную должность (роль), с которой он и получает некоторый типовой набор прав и полномочий.

Таким образом, политика разграничения доступа в компьютерных системах, автоматизирующих те или иные организационно-технологические или организационно-управленческие процессы, должна строиться на основе функционально-ролевых отношений, складывающихся в предметной области компьютерной системы.

Несколько позже появились и формальные выражения ролевых основ управления доступом (Role-Based Access Control — RBAC).

Основой ролевых моделей, как отмечалось, является введение в субъектно-объектную модель компьютерных систем дополнительной категории активных сущностей — ролей. Можно дать следующее формальное определение роли.

Ролью называется активно действующая в компьютерной системе абстрактная сущность, обладающая логически взаимосвязанным набором полномочий, необходимых для выполнения определенных функциональных обязанностей пользователями системы.

Приведем формальную спецификацию ролевой модели разграничения доступа.

1. Компьютерная система представляется совокупностью следующих множеств:

- множества пользователей *S*;
- множества ролей *R*;
- множества полномочий *P*;

– множества сеансов C работы пользователей с системой.

Множество полномочий P в общем виде задается специальными механизмами, объединяющими операции доступа и объекты доступа, например, запросами на обработку данных в СУБД, или иными именованными процедурами обработки данных, в том числе возможно высокого логического уровня.

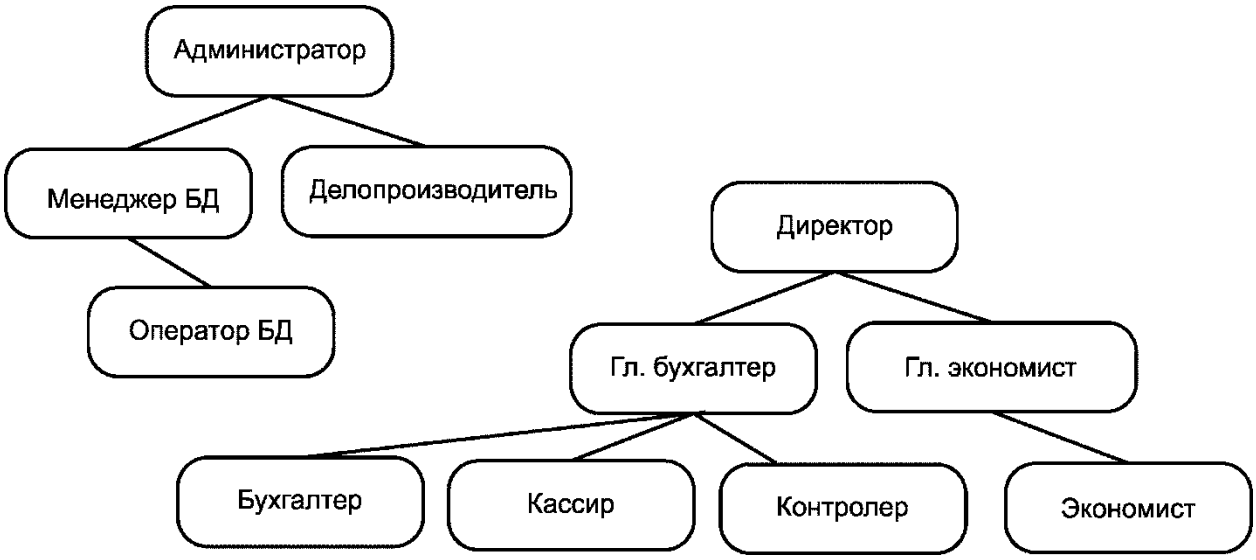
2. Ролевые отношения устанавливаются следующими отображениями множеств сущностей системы:

F_{PR}: $P \times R$ — отображение множества полномочий на множество ролей;

F_{SR}: $S \times R$ — отображение множества пользователей на множество ролей.

Иерархическая система ролей является наиболее близкой к реальным организационно-технологическим и организационно-управленческим схемам на предприятиях и в организациях. Должности сотрудников предприятий, организаций в большинстве случаев образуют иерархически подчиненные структуры. На рисунке представлены примеры иерархической системы ролей-должностей.

При этом помимо управленческого аспекта подчиненность ролей в большинстве случаев включает наследование прав и полномочий. В иерархически организованных структурах возможны два направления наследования полномочий и прав — «снизу» и «сверху».



При наследовании «сверху» подчиненный субъект помимо своих индивидуальных (так называемых явных) прав и полномочий получает (наследует) права и полномочия родителей. Подобный подход широко применяется в организации доступа к объектам, образующим иерархически организованную структуру, а также в системах индивидуально-группового доступа.

Модели с иерархически организованными ролями основаны на механизме наследования «снизу», при котором старшая в иерархии роль получает (владеет) права и полномочия непосредственно подчиненных ролей и т. д.

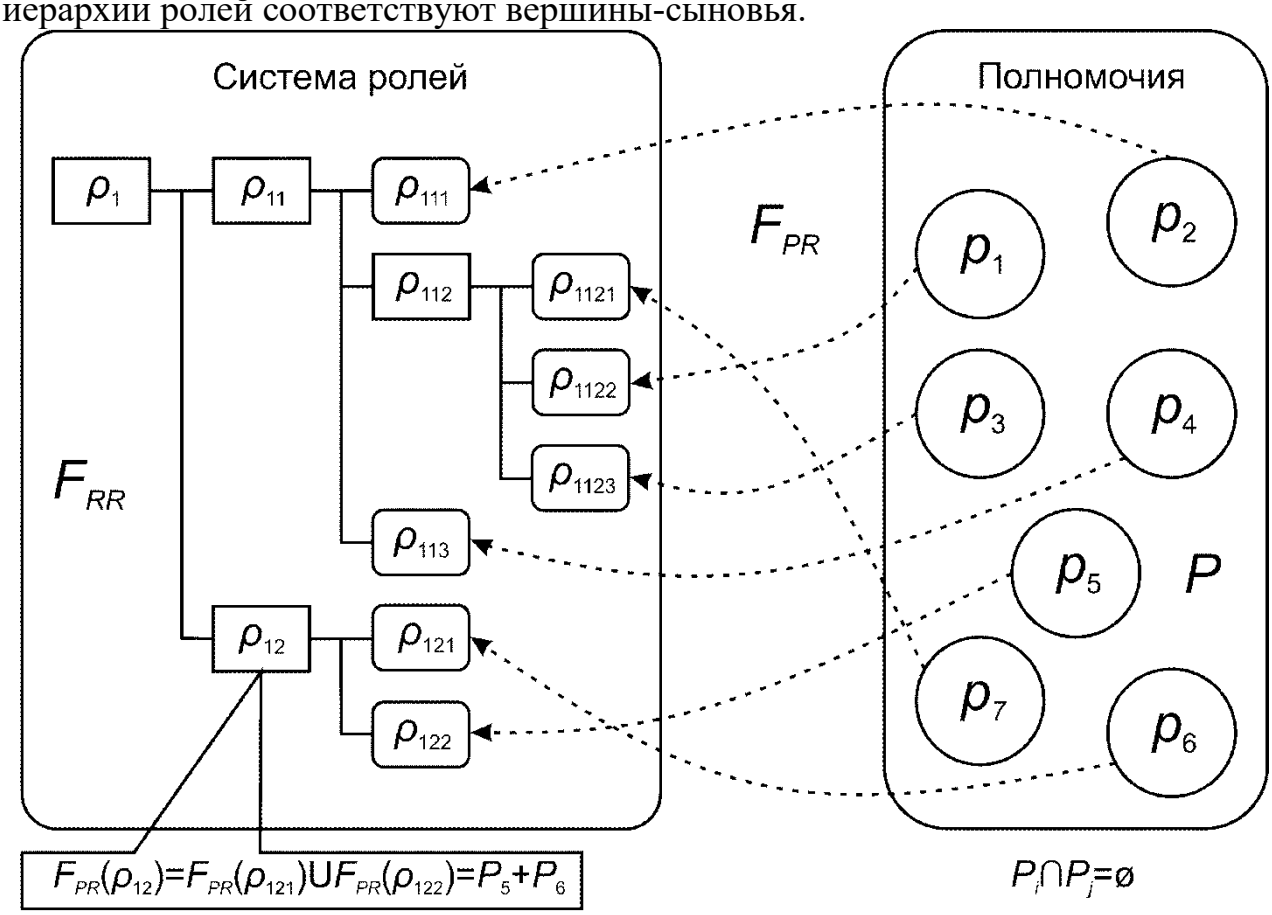
В иерархической системе ролей все множество полномочий разбивается на непересекающиеся подмножества, назначаемые отношением F_{PR} листовым ролям корневого графа иерархии ролей:

$F_{PR}(p_j) = \{p_{j1}, p_{j2}, p_{j3}, \ldots\}$.

$F_{PR}(p_j) \cap F_{PR}(p_i) \cap \ldots = \varnothing$.

$F_{PR}(p_j) \cup F_{PR}(p_i) \cup \ldots = P$.

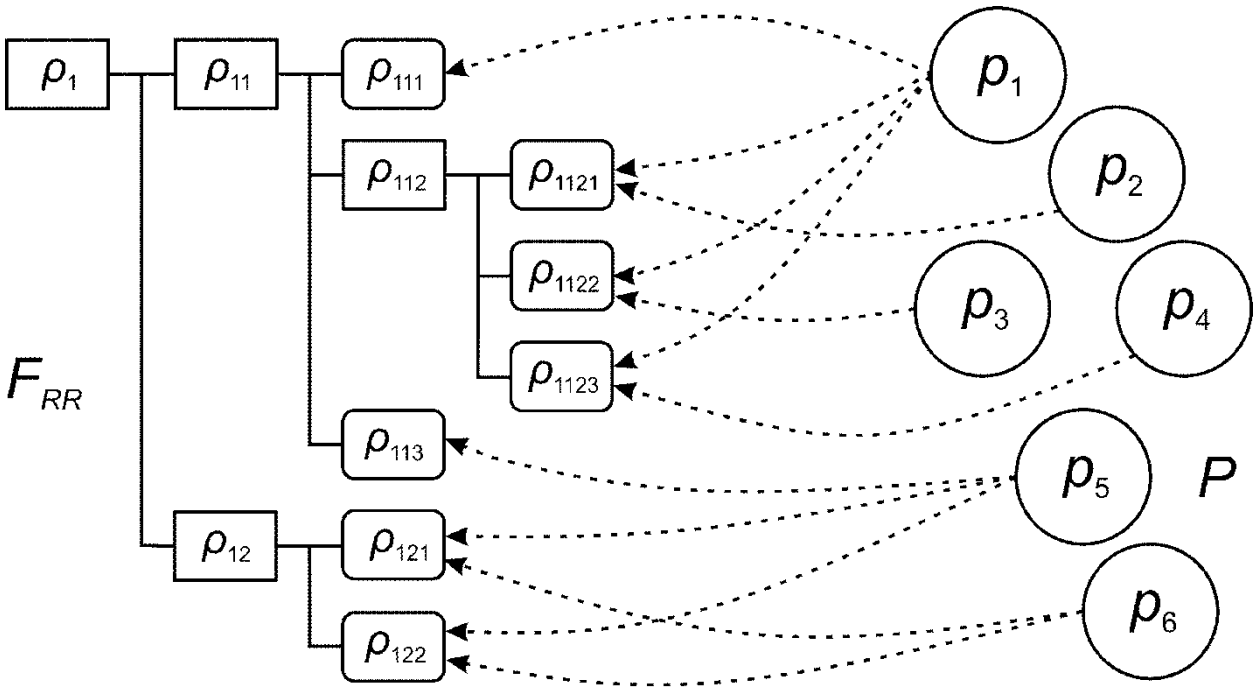
Полномочия старших ролей, т. е. ролей, которым соответствуют внутренние вершины корневого графа иерархии ролей, определяются как объединение прав и полномочий непосредственно подчиненных ролей, которым в графе иерархии ролей соответствуют вершины-сыновья.



В практическом применении ролевые модели позволяют существенно упростить проектирование и администрирование систем разграничения доступа для компьютерных систем, автоматизирующих сложные, нетривиальные организационно-технологические и организационно-управленческие схемы и процессы. Вместе с тем, в ролевых моделях нет строгих доказательств безопасности системы в соответствии с определенными формализованными критериями. Поэтому их безопасность основывается на контрольных механизмах дискреционных или мандатных моделей, средствами которых регулируется доступ ролевых субъектов к объектам системы.

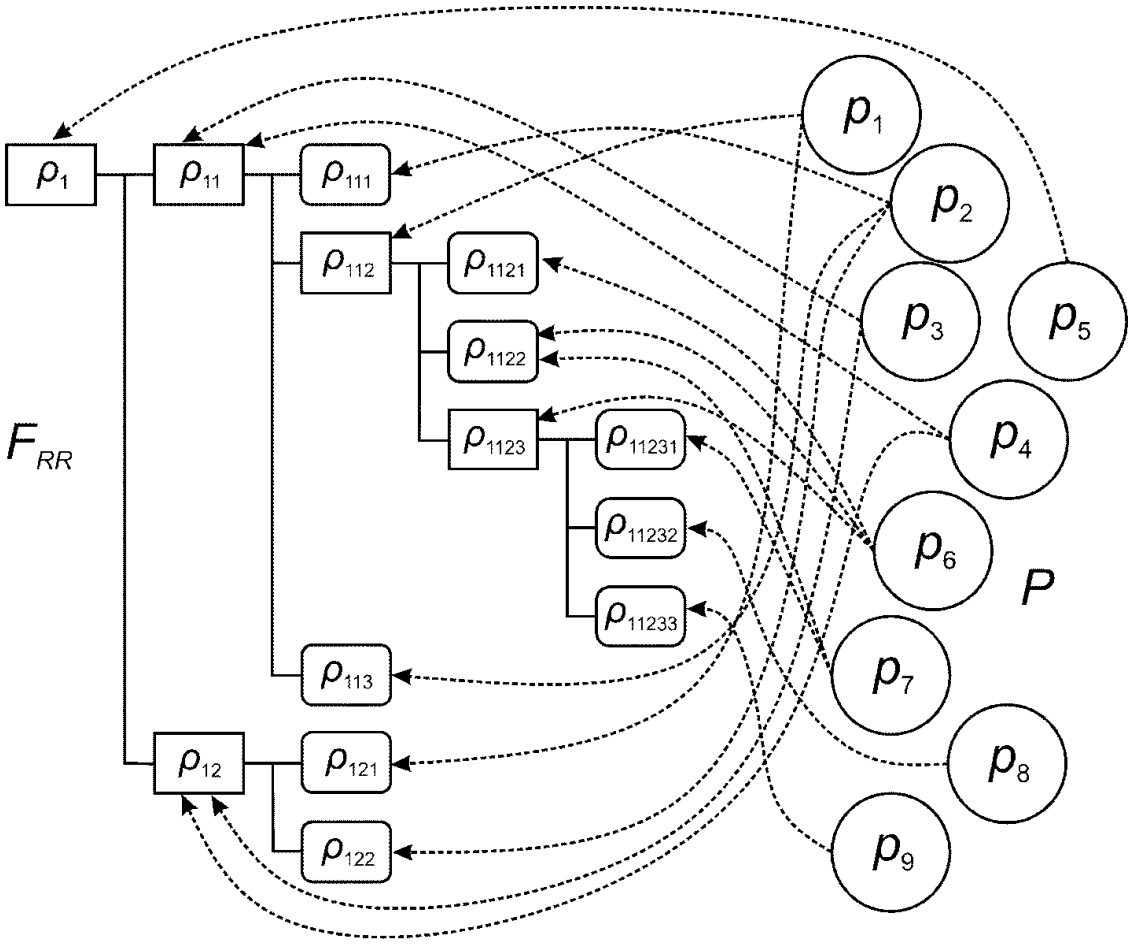
Задания

1. Пусть имеется система иерархически организованных ролей R ($\rho \in R$), представленная на рисунке. Ролям назначены полномочия из конечного множества P ($p \in P$).



Определить полномочия ролей: ρ_{112}, ρ_{12}, ρ_{11}.

2. Пусть имеется система иерархически организованных ролей R ($\rho \in R$), представленная на рисунке. Ролям назначены полномочия из конечного множества P ($p \in P$).



Определить полномочия ролей: ρ_{112}, ρ_{12}, ρ_{11}.

3. При предположении, что определенные полномочия могут быть назначены только ролям определенного уровня иерархии, определить возможный порядок (отношение доминирования) на множестве полномочий. Другими слова следует определить уровни полномочий для системы иерархически организованных ролей представленных на предыдущем рисунке.

Контрольные вопросы

1. Какие основные проблемы задания правил изменения иерархии ролей рассматриваются в модели администрирования ролевого управления доступом?
2. Что такое «роль»?
3. Что называется иерархией ролей в базовой модели ролевого управления доступом?
4. Перечислите основные элементы модели *RBAC*.
5. Какого вида ограничения, описанные в базовой модели ролевого управления доступом, могут быть использованы при определении требований либерального или строгого мандатного управления доступом?

Практическая работа № 7

Применение теории графов для моделирования систем защиты информации

Цель работы: овладение навыками создания математических моделей для решения профессиональных задач в области защиты информации.

Теоретические сведения

В процессе проектирования сложных систем, таких как комплексные и интегрированные системы защиты информации информационных систем (ИС), в большинстве случаев прибегают к моделированию основных процессов, происходящих внутри системы и на стыке среда-система. Кроме того, модели могут использоваться для проведения мониторинга и аудита безопасности на этапах эксплуатации и сопровождения ИС.

Под моделированием здесь понимаются математическое моделирование, позволяющее получить формальное описание системы и производить в дальнейшем количественные и качественные оценки ее показателей. В основу моделей системы защиты информации может быть положена теория графов.

Отличия большинства моделей заключаются в том, какие параметры они используют в качестве входных, а какие — представляют в виде выходных после проведения расчетов. Кроме того, в последнее время широкое распространение получают методы моделирования, основанные на неформальной теории систем: методы структурирования, методы оценивания и методы поиска оптимальных решений. Методы структурирования являются развитием формального описания, распространяющимся на организационно-технические системы. Использование этих методов позволяет представить архитектуру и процессы функционирования сложной системы в виде, удовлетворяющем следующим условиям:

- полнота отражения основных элементов и их взаимосвязей;
- простота организации элементов и их взаимосвязей;
- гибкость — простота внесения изменений в структуру и т. д.

Методы оценивания позволяют определить значения характеристик системы, которые не могут быть измерены или получены с использованием аналитических выражений, либо в процессе статистического анализа, — вероятности реализации угроз, эффективность элемента системы защиты и других. В основу таких методов положено экспертное оценивание — подход, заключающийся в привлечении специалистов в соответствующих областях знаний для получения значений некоторых характеристик. Методы поиска оптимальных решений представляют собой обобщение большого количества самостоятельных, в большинстве своем математических теорий с целью решения задач оптимизации. В общем случае к этой группе можно также отнести методы неформального сведения сложной задачи к формальному описанию с последующим применением формальных подходов.

Математическая теория графов имеет несколько приложений к моделированию системы защиты информации. Это, например, графы атак. Неформально граф атаки — это граф, представляющий все возможные последовательности действий нарушителя для реализации угрозы. Такие последовательности действий называются путями атак.

Принцип «разумной достаточности» является базой минимизирующего затраты от происшествий в сфере информационной безопасности подхода управления рисками. Вариант риск-ориентированной модели, использующей теорию графов это граф угроз. В этом случае система защиты информации представляется в виде ориентированного графа, где вершинами, будут угрозы активам со стороны злоумышленников, а дугами — их связи. При этом каждая дуга будет обозначать связь угрозы с угрозой, вероятная реализация которой является прямым следствием реализации другой угрозы.

С помощью графов можно построить модель переходов состояний объекта защиты при воздействии угроз безопасности.

Краткие сведения из теории графов

Простым графом G называется пара множеств (V, E), где V — не пустое, конечное множество элементов, называемых вершинами. Графически это множество изображается точками; E — конечное множество неупорядоченных пар различных элементов из V, называемых ребрами. Графически это множество изображается линией, соединяющей пару точек.

Ориентированным графом (орграфом) G называется пара (V,E), где V — не пустое, конечное множество элементов (вершин); E — конечное семейство упорядоченных пар элементов из V, называемых дугами.

Другими словами, граф — система, которая может быть рассмотрена как множество кружков и множество соединяющих их линий (геометрический способ задания графа см. на рис. 3). Кружки называются вершинами графа, линии со стрелками — дугами, без стрелок — ребрами. Граф, в котором направление линий не выделяется (все линии являются ребрами), называется *неориентированным*; граф, в котором направление линий принципиально (линии являются дугами), называется *ориентированным*.

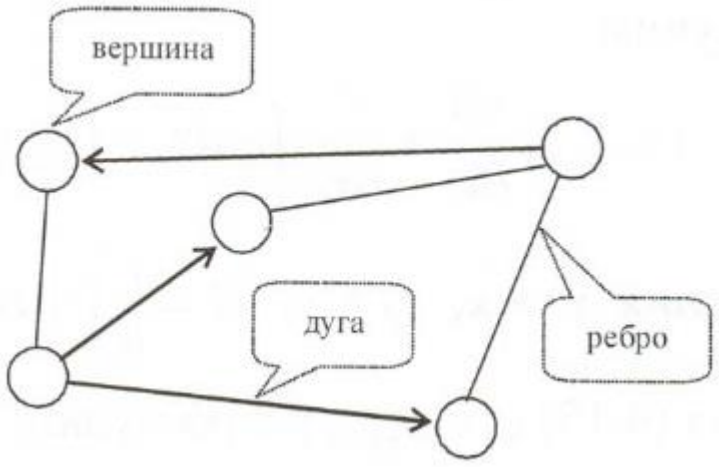


Рис. 3. Графическое представление графа

Смежность вершин графа — это когда две вершины графа соединены ребром.

Матрица смежности, как и матрица инцидентности, позволяет установить множество вершин, соседних с заданной (то есть рассматриваемой в конкретной задаче), не прибегая к полному просмотру всей матрицы. Матрицы смежности обычно представляются двумерным массивом размера $n \times n$, где n — число вершин графа.

Матрица смежности S — это квадратная матрица, в которой и число строк, и число столбцов равно n — числу вершин графа. В ячейки матрицы смежности записываются некоторые числа в зависимости от того, соединены соответствующие вершины ребрами или нет, и от типа графа.

Матрица смежности для неориентированного графа

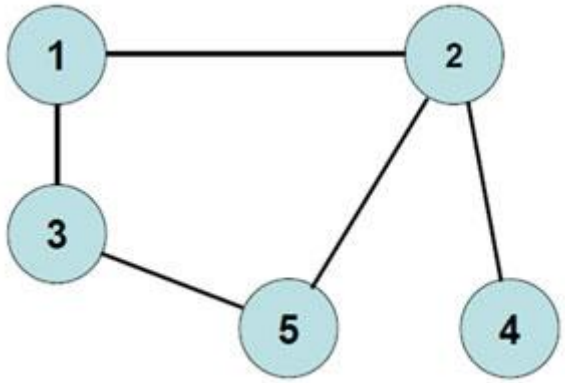
Элемент матрицы смежности s_{ij} неориентированного графа определяется следующим образом:

– равен единице, если вершины v_i и v_j смежные;

– равен нулю, если вершины v_i и v_j не смежные.

Если для элемента матрицы v_{ij} имеет место $i = j$, т. е. элемент находится на диагонали, то этот элемент равен единице, если этот элемент имеет петлю, и нулю, если элемент не имеет петли.

Пример 1. Составить **матрицу смежности** для графа, представленного на рисунке ниже.



Ответ.

V	1	2	3	4	5
1	0	1	1	0	0
2	1	0	0	1	1
3	1	0	0	0	1
4	0	1	0	0	0
5	0	1	1	0	0

Таким образом, ***матрица смежности*** неориентированного графа симметрична относительно главной диагонали.

Матрица смежности для ориентированного графа

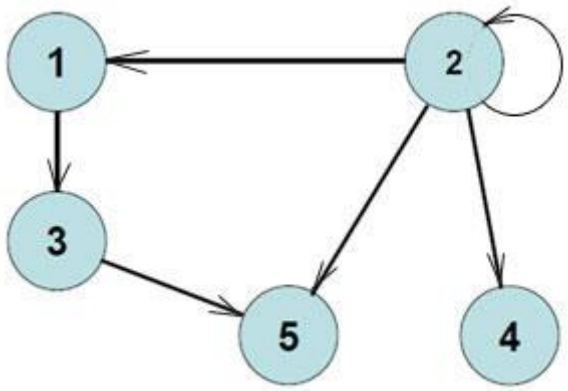
Элемент матрицы смежности s_{ij} ориентированного графа определяется следующим образом:

– равен единице, если из вершины v_i в вершину v_j входит дуга;

– равен нулю, если из вершины v_i в вершину v_j дуга не входит.

Как и для неориентированных графов, так и для ориентированных, если для элемента матрицы v_{ij} имеет место $i = j$, т. е. элемент находится на диагонали, то этот элемент равен единице, если этот элемент имеет петлю, и нулю, если элемент не имеет петли.

Пример 2. Составить **матрицу смежности** для графа, представленного на рисунке ниже.



Ответ.

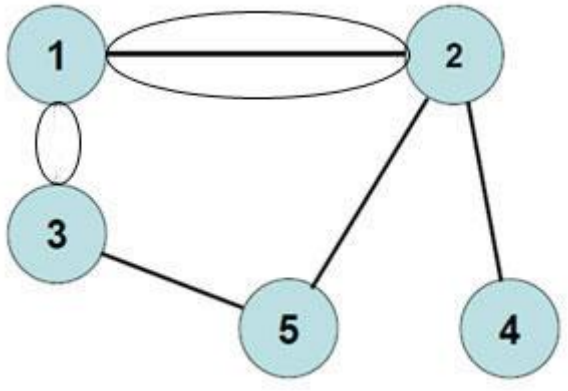
V	1	2	3	4	5
1	0	1	0	0	0
2	0	1	0	0	0
3	1	0	0	0	0
4	0	1	0	0	0
5	0	1	1	0	0

Таким образом, ***матрица смежности*** ориентированного графа не симметрична.

Матрица смежности для графа с кратными ребрами

Если в графе есть вершины, соединенные между собой несколькими ребрами, то элемент матрицы смежности s_{ij} равен числу ребер, соединяющих вершины v_i и v_j. Из этого следует, что если вершины v_i и v_j не соединены ребрами, то элемент матрицы смежности s_{ij} равен нулю.

Пример 3. Составить **матрицу смежности** для графа, представленного на рисунке ниже.



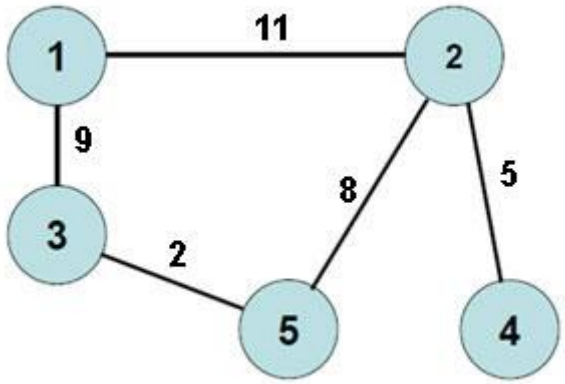
Ответ.

V	1	2	3	4	5
1	0	3	2	0	0
2	3	0	0	1	1
3	2	0	0	0	1
4	0	1	0	0	0
5	0	1	1	0	0

Матрица смежности для взвешенного графа

В случае взвешенного графа элемент матрицы смежности s_{ij} равен числу w, если существует ребро между вершинами v_i и v_j с весом w. Элемент s_{ij} равен нулю, если ребер между вершинами v_i и v_j не существует.

Пример 4. Составить **матрицу смежности** для графа, представленного на рисунке ниже.



Ответ.

V	1	2	3	4	5
1	0	11	9	0	0
2	11	0	0	5	8
3	9	0	0	0	2
4	0	5	0	0	0
5	0	8	2	0	0

Порядок выполнения работы

Имеется ориентированный граф, узлами которого являются состояния объекта защиты, а дугами — переходы из одних состояний объекта защиты в другие. Граф представлен матрицей смежности (табл. 10), а всякой дуге, исходящей из любого узла, приписаны:

– вероятности реализации угрозы объекту защиты при переходе в смежный узел ($P_{угр}$);

– цена средств защиты (в условных единицах), нейтрализующих угрозу перехода между смежными узлами ($Ц_{сз}$);

– время перехода состояния объекта защиты (в минутах) между смежными узлами (t_{ij}).

Таблица 10

Матрица смежности: элемент матрицы $a_{ij} = (P_{угр}; Ц_{сз}; t_{ij})$

0	0.7; 15; 08	0.8; 25; 15	0.6; 16; 12	0.5; 32; 06	0.1; 05; 04
0.7; 12; 08	0	0.2; 02; 10	0.6; 30; 02	0.7; 12; 11	0.4; 08; 14
0.8; 40; 15	0.2; 15; 10	0	0.9; 35; 04	0.8; 60; 15	0.6; 40; 02
0.6; 15; 12	0.6; 25; 02	0.9; 58; 04	0	0.8; 45; 11	0.4; 60; 04
0.5; 15; 06	0.7; 25; 11	0.8; 45; 15	0.8; 90; 11	0	0.2; 15; 16
0.1; 05; 04	0.8; 60; 14	0.6; 55; 02	0.4; 12; 04	0.2; 10; 16	0

Необходимо произвести анализ объекта защиты, а именно:

1. В соответствии с заданными исходными данными построить граф.

2. Определить (расположив по возрастанию) все реализуемые пути между указанными узлами согласно индивидуальному варианту (табл. 10) с точки зрения вероятности реализации угроз для объекта защиты. По результатам моделирования сформулировать выводы.

3. Определить минимальную и максимальную стоимости средств защиты при реализации указанной траектории пути согласно индивидуальному варианту (табл. 11). По результатам моделирования сформулировать выводы.

4. Определить минимальное и максимальное время перехода состояния объекта защиты между указанными узлами согласно индивидуальному варианту (табл. 11). По результатам моделирования сформулировать выводы.

Варианты заданий

Таблица 11

Узлы в исследуемом графе

№	Узлы	№	Узлы
1.	1,2	9.	2,6
2.	1,3	10.	3,4
3.	1,4	11.	3,5
4.	1,5	12.	3,6
5.	1,6	13.	4,5
6.	2,3	14.	4,6
7.	2,4	15.	5,6
8.	2,5		

Контрольные вопросы

1. Перечислить математические методы, используемые для моделирования систем защиты.

2. Пояснить, что такое адекватность математических моделей.

3. Перечислить и объяснить основные виды представления графов.

4. Объяснить алгоритм поиска кратчайших путей в графе.

5. Объяснить метод прямого построения кратчайших остовых деревьев.

Список рекомендуемой литературы

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М. : Яхтсмен, 1996. 192 с.

2. Гайдамакин Н.А. Теоретические основы компьютерной безопасности : учеб. пособие. Екатеринбург : Изд-во Урал. ун-та, 2008. 212 с.

3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. М. : Феникс, 2008. 173 с.

4. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / под ред. А.С. Маркова. М. : Радио и связь, 2012. 192 с.

5. Теория графов: метод. указания к самостоят. работе для студентов матем. и экон. специальностей / сост. В.Д. Власенко. Хабаровск : Изд-во Хабар. гос. техн. ун-та, 2005. 23 с.

6. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации : учеб. пособие. Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. 196 с.

Учебное электронное издание

Бусько Михаил Михайлович

БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Методические указания по выполнению практических работ

Подписано в пользование 05.06.20. Объем данных 1,33 Мб.
ИД № 06318 от 26.11.01.
Научное издательство Байкальского государственного университета.
664003, г. Иркутск, ул. Ленина, 11.
http://bgu.ru.