**Лабораторная работа № 4-5**

**Методы выбора мероприятий по повышению уровня ИБ**

**Цель занятия:** получить практические навыки применения математических методов для выбора мероприятий по повышению уровня информационной безопасности в организации.

**1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

В процессе проведения аудита информационной безопасности (ИБ) аудитор может предложить комплекс мер (вариантов) для повышения уровня ИБ (<https://selectel.ru/blog/infobez-2024-review/>):

1. Использование актуальных версии ОС и ПО – регулярно следить за актуальностью используемых версий ОС и ПО. При появлении стабильных версий планируйте обновление и реализацию совместимости с имеющейся инфраструктурой.

2. Понимание цели каждого опубликованного в интернет порта. Любая публикация порта в открытую сеть повышает риски нарушения безопасности публикуемого ресурса и всей инфраструктуры. Публикуйте ресурсы, только если вы убедились в реальной необходимости и предварительно настроили средства защиты.

3. Не публиковать порты для управления устройствами и хостами. Если требуется удаленное подключение к хостам для управления, лучший вариант — настройка VPN. Допустимый вариант — ограничение адресов для доступа к портам управления с помощью файрвола. Следите за открытыми портами. Настройте сканирование портов, чтобы быть в курсе публикации новых служб в интернет. Вы можете пользоваться бесплатным мониторингом портов от Selectel.

4. Разнесение веб-приложений и сторонних сервисы на различные хосты. Разделите web-часть вашего приложения и остальные сервисы по различным хостам. Используя межсетевой экран, пропишите четкие правила доступа для каждого сервиса.

5. Использование более безопасных версий протоколов. Например, HTTPS вместо HTTP, SMTPS вместо SMTP, FTPS вместо FTP, SSH вместо TELNET, SNMPv3 вместо SNMP первой и второй версий.

6. Использование reverse-proxy в DMZ для публикаций веб-приложений. Вот [перечень актуальных HTTP-заголовков](https://owasp.org/www-project-secure-headers/), которые можно использовать для повышения уровня защищенности. Публиковать ресурсы можно, например, с помощью nginx (engine x — произносится как энджи́нкс — веб-сервер), настроив параметры HTTP-заголовков.

7. Использование Port-Forwarding (технология, которая позволяет обращаться из Интернет к компьютеру во внутренней сети за маршрутизатором, использующим NAT (Network Address Translation, трансляция сетевых адресов — функция для изменения IP-адреса во время передачи пакетов Ethernet через маршрутизатор). Доступ осуществляется при помощи перенаправления трафика определенных портов с внешнего адреса маршрутизатора на адрес выбранного компьютера в локальной сети) для проброса портов вместо NAT.

8. Использование fail2ban (программа для защиты серверов от атак методом грубой силы. Написанная на языке программирования Python) для сервисов, в которых настроена авторизация. Например, вот [информация о настройке fail2ban для SSH](https://putty.org.ru/articles/fail2ban-ssh).

9. Использование, по возможности, SSH-ключи для авторизации (Secure SHell — «безопасная оболочка» — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений, например, для передачи файлов).

10. Авторизация на хостах происходит под непривилегированной учетной записью с дальнейшим повышением прав.

11. Использование сложных паролей. Например, пароли со следующими характеристиками: длина не менее 15 символов с алфавитом, содержащим строчные, заглавные буквы, цифры, спецсимволы.

12. Использование авторизацию по сертификату, если требуется ограничить доступ к публикациям портов понятному конечному числу пользователей. Реализация возможна, например, с помощью nginx в качестве обратного прокси-сервера для публикации ресурсов.

13. Использование решений IDS/IPS. Intrusion Detection System — система обнаружения вторжений. IPS, Intrusion Prevention System, — система предотвращения вторжений. По сравнению с традиционными средствами защиты (антивирусами, спам-фильтрами, файерволами) IDS/IPS обеспечивают гораздо более высокий уровень защиты сети. Можно использовать open source-решения (Suricata, Snort) или, например, обеспечить защиту сервисов через провайдера. Подобные решения есть и у Selectel — аренда межсетевых экранов и аттестованный ЦОД.

14. По возможности использование двухфакторной аутентификации.

15. Использование WAF (Web application firewall) – совокупность мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение. WAF относятся к прикладному уровню модели OSI (Open Systems Interconnection model — сетевая модель стека (магазина) сетевых протоколов OSI/ISO, с ее помощью различные сетевые устройства могут взаимодействовать друг с другом).

16. Использование фильтрации GeoIP (система учета географической принадлежности IP-адресов). Для ограничения пула IP-адресов, которым разрешен доступ к критическим ресурсам, можно использовать фильтрацию по GeoIP на основе списка стран с целевой аудиторией для подключения. Однако этот подход не сработает, если атакующая сторона использует прокси-серверы в разрешенных странах или ваши пользователи могут использовать IP, которые принадлежат компаниям в заблокированных странах. Также многие файрволы поддерживают эту функциональность — например, UserGate (можно арендовать в Selectel) и pfSense (можно установить на виртуальный или выделенный сервер).

17. Подключение защиты от DDOS-атак. Так повышается доступность вашего сервиса путем защиты от DDoS-атак. Все клиенты Selectel получают защиту от самых распространенных DDoS-атак.

18. Настройка регулярного сканирования белых IP-адресов. Регулярное внешнее сканирование ресурсов поможет поддерживать безопасность на высоком уровне. Можно развернуть свой хост для сканирования или воспользоваться услугой Selectel по анализу уязвимостей.

19. Отслеживание информации о новых уязвимостях. Актуальную информацию можно получить, например, из следующих источников:

– банк данных угроз безопасности информации (ФСТЭК),

– National Vulnerability Database,

– Common Vulnerabilities And Exposures,

– VulnDB – Vulnerability Intelligence.

20. Настройка логирования и мониторинга ИБ. Необходимо настроить сбор логов межсетевого экрана, систем обнаружения и предотвращения вторжения, логи сервисов и ОС. Для более эффективного реагирования должна быть настроена корреляция всей собранной информации. Для мониторинга информационной безопасности можно использовать open source-решение, например Wazuh (это бесплатная опенсорс-платформа с XDR и SIEM для защиты конечных устройств (End Devices), облачных и локальных сред), или воспользоваться «коробочным» решением, существующим на рынке

Эти и другие решения (альтернативы) могут иметь различные значения определенных характеристик (критериев), по которым можно осуществить выбор наиболее подходящей для данной организации. Если альтернатив и критериев немного (два-три), то этот выбор еще можно как-то примерно оценить без использования математических методов. На практике альтернатив и критериев много. Кроме того, альтернативы часто не имеют выраженного лидера и отличаются друг от друга по значениям критериев в ту или иную сторону незначительно (недоминируемые альтернативы). Поэтому здесь целесообразно применение аппарата нечеткой логики (fuzzy logic).

В обычной логике функция принадлежности μ объекта к какому либо классу объектов имеет два значения – «Истина» и «Ложь», например, если есть угроза ИБ, то μ=1, если нет, то μ=0. В нечеткой логике μ может принимать значения в диапазоне от 0 до 1, причем эти значения определяет человек, руководствуясь своими субъективными соображениями. Например, на вопрос о том, является ли данное воздействие опасным с точки зрения ИБ человек может сказать, что является с μ=0.8 – то есть нельзя утверждать, что однозначно опасно с μ=1, но все же 0.8 ближе к 1, обозначающей «опасное воздействие», чем к 0, который характеризует полную безопасность воздействия. В этом, кстати, кроется главный недостаток нечеткой логики – субъективизм в оценке μ, однако, она дает возможность принимать решения в условиях неопределенности и нечеткости исходных данных.

В условиях неопределенности и наличии многих альтернатив решения задачи по обеспечению ИБ, приходится применять математические методы для выбора альтернатив и автоматизировать расчеты с помощью создания соответствующих программных средств.

В данной лабораторной работе представлены два метода выбора альтернатив: на основе пересечения нечетких множеств и на основе недоминируемых альтернатив.

Рассмотрим первый способ выбора альтернатив решений по ИБ, каждая из которых характеризуется различными критериями.

**Метод многокритериального выбора альтернатив на основе пересечения нечётких множеств**.

Пусть иметься некоторое множество A={a1, a2, …, am} альтернативных решений в области ИБ (например, из списка 20 вариантов, представленного выше), где aj – отдельные альтернативы, j=1, …, m. Есть множество критериев C={C1, C2, …, Cn} по которым мы оцениваем эти альтернативы, где Ci – отдельные критерии, i=1, …, n.

Экспертным путем задаются оценки альтернатив по каждому i-му критерию, которые можно представить нечеткими множествами вида:

 (1)

где μi(aj)–функция принадлежности j-й альтернативы по i-му критерию, принимающая значения от 0 (альтернатива совершенно не подходит по данному критерию) до 1 (альтернатива полностью подходит по данному критерию).

Для выбора лучшей альтернативы рассчитывается пересечение нечетких множеств, полученных по (1):

 (2)

Пересечение  реализуется как взятие **минимума** по столбцу для всех μi. Лучшей будет та альтернатива, которой соответствует **максимальное значение D** в (2). Если критерии имеют разную важность для аудитора, то им можно присвоить дополнительно весовые коэффициенты, отражающие эту важность.

**Пример.** Пусть исходные данные для выбора альтернативы представлены в таблице 1.

Таблица 1 – Исходные данные

|  |  |  |  |
| --- | --- | --- | --- |
|  | Альтернатива 1 | Альтернатива 2 | Альтернатива 3 |
| Критерий 1(чем больше его значение, тем лучше) | 20 | 21 | 18 |
| Критерий 2 (чем больше его значение, тем лучше) | 20 | 17 | 19 |
| Критерий 3(чем меньше его значение, тем лучше) | 12 | 10 | 11 |

**Решение.** Найдем значения μi для (1). Для определенности расчетов и возможности проверки ответов применим не экспертные оценки, а «метод пропорций», в котором лучшей альтернативе присваивается значение μi=1, а остальные рассчитываются с помощью пропорции от этой единицы.

Для 1-го критерия (чем больше его значение, тем лучше) лучшая альтернатива №2, так как для нее критерий имеет значение 21. Примем 21 за «1», то есть μ1(а2) = 1 и найдем остальные функции принадлежности по правилу «пропорций». Обозначим x = μ1(а1). Для первой альтернативы составим пропорцию:

20 – х,

21 – «1»,

отсюда х= 0.952, то есть μ1(а1) = 0.952.

Аналогично для 3-й альтернативы x = μ1(а3): 18 – х, 21 – «1», откуда х=18/21= 0.857, то есть μ1(а3) = 0.857.

Аналогично для второго критерия: принимаем лучшую альтернативу №1 μ2(а1)=1, тогда μ2(а2)=0.85, μ2(а3) = 0.95.

Для 3-го критерия ситуация другая – он чем он меньше, тем лучше, поэтому лучшая альтернатива №2, она имеет значение критерия 10. Примем μ3(а2)=1. Тогда для 1-й альтернативы обозначим (1/x) = μ3(а1) и пропорцию запишем в виде:

10 – «1»;

12 – (1/х),

откуда 1/х=1.2, следовательно х=μ3(а1) 1/1.2=0.83. Аналогично найдем μс3(а3)= 0.917. В результате совокупность функций принадлежности (1) можно представить таблицей 2.

Таблица 2 – Функции принадлежности

|  |  |  |  |
| --- | --- | --- | --- |
|  | Альтернатива 1 | Альтернатива 2 | Альтернатива 3 |
| Критерий 1(чем больше его значение, тем лучше) | 0.952 | 1 | 0.857 |
| Критерий 2 (чем больше его значение, тем лучше) | 1 | 0.85 | 0.95 |
| Критерий 3(чем меньше его значение, тем лучше) | 0.83 | 1 | 0.917 |
| Результат пересечения по столбцам (min) | **0.83** | **0.85** | **0.857** |

В таблице 2 по столбцам находим **минимум** (операция пересечения нечетких множеств), это реализуется нахождение D по (2). Матрица-строка D записана в последней строке таблицы 2 жирным шрифтом. В нижней строке находим **максимум** (объединение нечетких множеств), он подчеркнут и находится в третьем столбце, следовательно, лучшей будет считаться «Альтернатива 3». Задача решена.

Рассмотрим второй способ выбора альтернатив – **метод многокритериального выбора недоминируемых альтернатив на основе нечёткого отношения предпочтения**.

Недоминируемые альтернативы характеризуются тем, что среди них нет явного лидера, все они имеют более-менее одинаковые функции принадлежности по разным критериям.

Этапы этого метода до (1) включительно аналогичны предыдущему методу, поэтому будем считать, что значения функций принадлежности по всем критериям и альтернативам получены. Применим метод к предыдущему примеру. Возьмем данные из таблицы 2 и занесем их в таблицу 3.

Таблица 3 – Функции принадлежности

|  |  |  |  |
| --- | --- | --- | --- |
|  | Альтернатива 1 | Альтернатива 2 | Альтернатива 3 |
| Критерий 1(чем больше его значение, тем лучше) | 0.952 | 1 | 0.857 |
| Критерий 2 (чем больше его значение, тем лучше) | 1 | 0.85 | 0.95 |
| Критерий 3(чем меньше его значение, тем лучше) | 0.83 | 1 | 0.917 |

Занесем данные таблицы 3 в матрицу R:

 (3)

На основе R проводим попарное сравнение альтернатив по каждому критерию. Попарное сравнение легче проводить, чем когда сразу надо оценивать много вариантов. В данном случае дано три критерия → из R получим три матрицы используя выражение:

 (4)

Здесь через a и b обозначены сравниваемые элементы R. Используя (4) рассчитываются элементы квадратных матриц MR1, MR2, MR3. Количество этих матриц будет равно количеству критериев, а в каждой из этих матриц количество строк (столбцов) будет равно количеству альтернатив.

Пример рассмотрим в предположении, что R задана в (3). Вначале сформируем матрицу MR1. Она будет размера 3х3 идля ее формирования используется только 1-я строка (1).

Сразу по главной диагонали MR1 запишем единицы. Затем в 1-й строке (3) обозначим a=0.952, b=1. Так как 0.952<1, то работает вторая строка (4) и получаем 0. Далее a оставляем тем же, но b сдвигаем: b=0.857, получаем a=0.952> b=0.857, поэтому работает первая строка из (4) и результат будет 0.952–0.857=0.095. После такого прохода получили первую строку новой матрицы MR1: (1 0 0.095) – в ней первая 1 была установлена как принадлежащая главной диагонали.

Теперь продолжаем рассматривать первую строку из (3), но переходим ко второму столбцу: a=1. Назначаем b=0.952 – первый элемент строки. Выполняем аналогичные расчеты по (4). В данном случае a=1>b=0.952, следовательно, применяем 1-ю строку (4) и получаем: 1–0.952=0.048. Сдвигаем b на третий элемент строки b=0.857. В данном случае снова a=1>b=0.857, применяем 1-ю строку (4) и получаем 1 – 0.857=0.143. В итоге сформирована вторая строка матрицы MR1: (0.048 1 0.143).

Продолжаем рассматривать первую строку из (3), но переходим к третьему столбцу: a=0.857. Проводим аналогичные вышеизложенным расчеты. Но можно сразу увидеть, что этот элемент меньше остальных в строке, поэтому третья строка матрицы MR1: (0 0 1). В итоге получаем матрицу:

 (5)

Далее формируем матрицу MR2 рассматривая вторую строку в (3) и применяя (4). Расчеты аналогичны, поэтому приведем сразу вид этой матрицы:



Аналогично формируем матрицу MR3 рассматривая третью строку в (3):



Полученные матрицы «накладываем» друг на друга и «пробиваем» эту стопку матриц, выбирая в этой пробивке минимальный элемент в направлении, как показано на рисунке 1. Пробив так всю стопку получаем матрицу Q1.

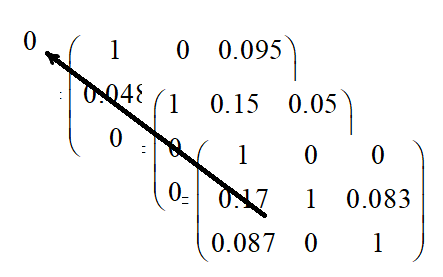


Рисунок 1 – Иллюстрация расчета элементов матрицы Q1

В нашем примере получим матрицу:



На основе матрицы Q1 проводится расчет матрицы-строки M\_nd по формуле:

 (6)

если Q1(j,i) < Q1(i, j,), то принимается Q1(j,i) – Q1(i, j,) = 0,

где sup – верхняя граница (максимальное значение), i,j – индексы элементов Q1.

Применим (6) к матрице Q1:

M\_nd(1) = 1 – sup(Q1(2,1)– Q1(1,2); Q1(3,1)– Q1(1,3))=1–sup(0–0;0–0)=1.

M\_nd(2) = 1 – sup(Q1(1,2)– Q1(2,1); Q1(3,2)– Q1(2,3))=1–sup(0–0;0–0)=1.

M\_nd(3) = 1 – sup(Q1(1,3)– Q1(3,1); Q1(2,3)– Q1(3,2))=1–sup(0–0;0–0)=1.

В результате получаем матрицу-строку: M\_nd = (1 1 1). Первый этап расчета закончен.

На втором этапе зададим весовые коэффициенты (задает специалист по своему усмотрению, в сумме значения весов должны давать 1), отражающие важность критериев в таблице 3 с точки зрения ИБ. Пусть w1=0.5, w2=0.4, w3=0.1. Формируем матрицу:

Q2=w1MR1+w2 MR2+ w3MR3,

которая в нашем случае принимает вид:





По Q2, аналогично как для Q1, по (6) рассчитываем матрицу-строку M\_Q2:

M\_Q2(1) = 1 – sup(Q2(2,1)–Q2(1,2); Q2(3,1)–Q2(1,3))=1–sup(0.041–0.06;0.0087–0.0675)= 1 – sup(0; 0)=1 – 0 = 1.

M\_Q2(2) = 1 – sup(Q2(1,2)– Q2(2,1); Q2(3,2)– Q2(2,3))=1– sup(0.06–0.041; 0.04–0.0798)= 1 – sup(0; 0)=1 – 0 = 1–sup(0.019; 0) = 1 – 0.019 = 0.981.

M\_Q2(3) = 1 – sup(Q2(1,3)–Q2(3,1); Q2(2,3)–Q2(3,2))=1– sup(0.0675–0.0087; 0.0798–0.04)= 1 – sup(0.0588; 0)=1 – 0 = 1–sup(0.019; 0.0398) = 1 – 0.0398= 0.9602.

В результате получаем матрицу-строку: M\_Q2= (1 0.981 0.9602).

На заключительном этапе находим матрицу-строку M как пересечение матриц-строк M\_nd и M\_Q2 используя операцию взятия минимума соответствующих элементов:

М =M\_nd  M\_Q2= (1 1 1)  (1 0.981 0.9602) = (1 0.981 0.9602).

В матрице М выбираем **максимальный** элемент – это 1, она является первым элементом, следовательно, по данному методу выбираем **первую** альтернативу.

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ**

**1.** Ниже представлена задача, которую надо решить двумя, описанными в теоретической части, методами:

– на основе пересечения нечетких множеств (значения весовых коэффициентов не учитывать);

– на основе методы выбора недоминируемых альтернатив с использованием нечеткого отношения предпочтения (значения весовых коэффициентов учитывать). Номер задачи выбрать в соответствии с номером варианта (по номеру фамилии в списке журнала группы) из таблицы 4.

Таблица 4 – Выбор номера задачи

|  |  |
| --- | --- |
| № фамилии по списку в журнале группы | № задачи |
| 1 – 5 | 1 |
| 6 – 10 | 2 |
| 11 – 20 | 3 |

*Задача 1***.** Выбрать наиболее подходящее решение для повышения уровня ИБ в организации на основе трех критериев: количество ролей пользователей информационной системы (чем больше, тем лучше), количество подключаемых проверок антивирусной системы (чем больше, тем лучше), стоимость приобретения и сопровождения (чем меньше, тем лучше). Cтепень значимости критериев принять: w1=0.5, w2=0.4, w3=0.1. При подсчете значений функции принадлежности использовать метод пропорций. Исходные данные приведены в таблице. **В ответе указать** номер выбранной альтернативы по каждому методу, матрицы D, M\_nd и M\_Q2.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Альтернатива 1 | Альтернатива 2 | Альтернатива 3 |
| количество ролей пользователей ИС (↑) | 15 | 20 | 30 |
| количество подключаемых проверок антивирусной системы(↑) | 10 | 10 | 5 |
| стоимость приобретения и сопровождения (↓),тыс. $ | 1 | 2 | 3 |

*Задача 2.*Выбрать наиболее подходящее решение для повышения уровня ИБ в организации на основе трех критериев: количество ролей пользователей информационной системы (чем больше, тем лучше), количество подключаемых проверок антивирусной системы (чем больше, тем лучше), стоимость приобретения и сопровождения (чем меньше, тем лучше). При подсчете значений функции принадлежности использовать метод пропорций. Степень значимости критериев принять: w1=0.5, w2=0.4, w3=0.1. Исходные данные приведены в таблице. **В ответе указать** номер выбранной альтернативы по каждому методу, матрицы D, M\_nd и M\_Q2..

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Альтернатива  1 | Альтернатива  2 | Альтернатива 3 | Альтернатива  4 |
| количество ролей пользователей ИС (↑) | 10 | 20 | 30 | 30 |
| количество подключаемых проверок антивирусной системы(↑) | 10 | 15 | 5 | 10 |
| стоимость приобретения и сопровождения (↓),тыс. $ | 2 | 1 | 3 | 4 |

*Задача 3.*Выбрать наиболее подходящее решение для повышения уровня ИБ в организации на основе двух критериев: количество подключаемых проверок антивирусной системы (чем больше, тем лучше), стоимость приобретения и сопровождения (чем меньше, тем лучше). При подсчете значений функции принадлежности использовать метод пропорций. Степень значимости критериев принять: w1=0.6, w2=0.4. Исходные данные приведены в таблице. **В ответе указать** номер выбранной альтернативы по каждому методу, матрицы D, M\_nd и M\_Q2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Технология | Альтернатива  1 | Альтернатива  2 | Альтернатива  3 | Альтернатива  4 |
| количество подключаемых проверок антивирусной системы(↑) | 25 | 25 | 50 | 75 |
| стоимость приобретения и сопровождения (↓),тыс . руб. | 100 | 50 | 80 | 150 |

**1.2.** Написать программу, автоматизирующую расчеты по методу пересечения нечетких множеств.

Входные данные программы: таблица условия задачи. Значения весовых коэффициентов можно не учитывать.

Выходные данные: номер альтернативы и матрица D.

Рекомендуемая среда реализации – Python или MatLAB. Запустить программу с исходными данными задачи и сравнить результаты ее работы с результатами, полученными в п. 2.1.

**Контрольные вопросы**

1. Как можно обеспечить скрытность портов для управления устройствами и хостами?
2. Перечислите безопасные версий протоколов.
3. Что обозначает словосочетание Port-Forwarding?
4. Для чего испльзуются SSH-ключи?
5. К какому уровню модели OSI относится WAF?
6. В чем преимущество методов нечеткой логики в задачах принятия решений?

**Оформить отчет** о выполнении лабораторной работы в электронном виде, содержащий:

– индивидуальное задание;

– ручные расчеты по решению задачи в соответствии с номером варианта;

– текст программы, автоматизирующий решение задачи и результаты ее выполнения;

– вывод о совпадении результатов ручного и автоматизированного расчета.