Лабораторна робота 15-16

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ВИЗНАЧЕННЯ МІЦНОСТІ ЗАХИСТУ ІНФОРМАЦІ

Мета – дослідження процесів визначення міцності захисту інформації з використання різних моделей систем захисту інформації, дослідження процесів оцінки стійкості парольного захисту інформації

ТЕОРЕТИЧНІ ВІДОМОСТІ

15.1. Оцінка моделей систем захисту інформації

У загальному випадку найпростіша модель елементарного захисту будь-якого предмету може бути у вигляді представленому на рис. 15.1.

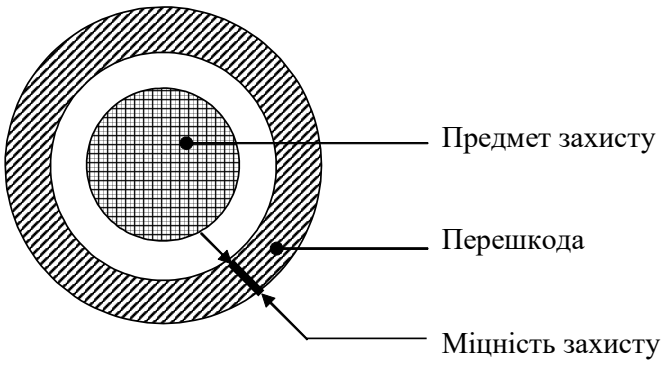

Рисунок 15.1 – Модель елементарного захисту

Якщо позначити імовірність неподолання перешкоди порушником через $P_{сзі}$, час життя інформації через $t_ж$, очікуваний час подолання перешкоди порушником через $t_{под}$, імовірність обходу перешкоди порушником через $P_{обх}$, то для випадку старіння інформації умову достатності захисту одержимо у виді наступних відношень:

$$P_{сзі}=1, \text{ якщо } t_ж<t_{под} \text{ і } P_{обх}=0,$$

де $P_{обх}$, яке рівне нулю, відбиває необхідність замикання перешкоди навколо предмету захисту. Якщо $t_ж > t_{под}$, а $P_{обх}=0$, то

$$P_{сзі}=(1-P_{под}), \qquad (15.1)$$

де $P_{под}$ - імовірність подолання перешкоди порушником за час, менший ніж $t_ж$.

Для реального випадку, коли $t_ж > t_{под}$ і $P_{обх} > 0$, міцність захисту можна представити у виді:

$$P_{сзі}=(1-P_{под})(1-P_{обх}),$$

де $P_{под}=0$, якщо $t_ж<t_{под}$, $P_{под}>0$, якщо $t_ж>t_{под.}$

Слід зазначити, що ця формула справедлива для випадку, коли порушників двоє, тобто коли один переборює перешкоду, а другий її обходить.

Припустимо, що порушник буде один і йому відомі міцність перешкоди і складність шляху її обходу. Оскільки одночасно по двох шляхах він йти не зможе, він вибере один з них – найбільш простий, тобто по формулі "або". Тоді формальний вираз міцності захисту в цілому для даного випадку буде відповідати формулі

$$P_{сзі}=\min\{(1-P_{под}),(1-P_{обх})\}. \quad (15.2)$$

Отже, міцність перешкоди після визначення і порівняння величин $(1 – P_{под})$ і $(1 – P_{обх})$ буде дорівнювати найменшому значенню однієї з них.

Вибір і визначення конкретної величини $P_{обх}$ спочатку можна проводити експертним шляхом на основі досвіду фахівців. Величина $P_{обх}$ повинна приймати значення від 0 до 1. При $P_{обх}=1$ захист втрачає всякий зміст.

Можливо також, що в однієї перешкоди може бути кілька шляхів обходу. Тоді формула (15.2) прийме вид:

$$P_{сзі}=\min\{(1-P_{под}),(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхк})\}, \quad (15.3)$$

де к – число шляхів обходу перешкоди.

Для випадку, коли порушників більше ніж один і вони діють одночасно (організована група) по кожному шляху, цей вираз з урахуванням сумісності подій буде мати вигляд:

$$P_{сзі}=(1-P_{под})(1-P_{обх1})(1-P_{обх2})(1-P_{обх3})...(1-P_{обхк}).$$

У цьому випадку, міцність перешкоди буде визначатись добутком результатів віднімання з одиниці значень ймовірності доступу порушників до предмету захисту по кожному можливому шляху подолання цієї перешкоди.

У тому випадку, коли інформація, що підлягає захисту, не застаріває або періодично обновляється, тобто коли нерівність $t_ж>t_{под}$ постійна або ж коли забезпечити $t_{под}>t_ж$ за будь-якими причинами неможливо, звичайно застосовується постійно діюча перешкода, що володіє властивостями виявлення і блокування доступу порушника до предмета або об'єкта захисту

Умову міцності перешкоди з виявленням і блокуванням НСД можна представити у виді співвідношення

$$\frac{T_{оп}+t_{спр}+t_в+t_{бл}}{t_{под}}<1, \quad (15.4)$$

де $T_{оп}$ – період опитування датчиків;

$t_{спр}$– час спрацьовування тривожної сигналізації; $t_в$– час визначення місця доступу;

$t_{бл}$– час блокування доступу.

Якщо позначимо суму $(T_{оп}+t_{спр}+t_в+t_{бл})$ через $T_{вбл}$, одержимо співвідношення:

$$\frac{T_{вбл}}{t_{под}}<1. \quad (15.5)$$

Процес контролю НСД і несанкціонованих дій порушника в часі представлений на рис. 15.2. З діаграми на рис. 15.2. зрозуміло, що порушник може бути не виявлений у двох випадках:

а) коли $t_{под} < T_{оп}$;

б) коли $T_{оп}< t_{под}< T_{вбл}$.

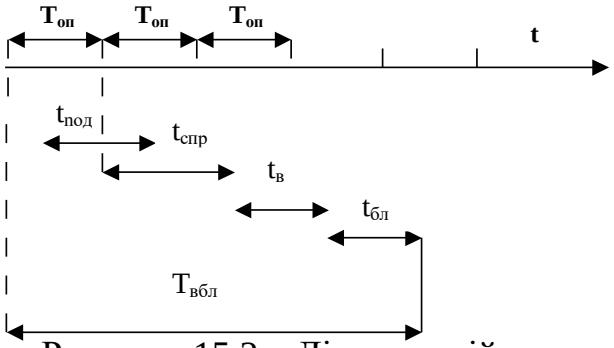

Рисунок 15.2 – Діаграма дій порушника

У першому випадку потрібна додаткова умова – влучання інтервалу часу $t_{под}$ в інтервал $T_{оп}$, тобто необхідна синхронізація дій порушника з частотою опитування датчиків виявлення. Для розв'язання цієї задачі порушникові прийдеться таємно підключити вимірювальну апаратуру в момент виконання несанкціонованого доступу до інформації, що є досить складною задачею для сторонньої людини. Тому вважаємо, що свої дії з частотою опитування датчиків він синхронізувати не зможе і може розраховувати лише на деяку ймовірність успіху, що виражається в імовірності влучення відрізка часу $t_{под}$ у проміжок часу між імпульсами опитування датчиків, рівний $T_{оп}$.

Відповідно до визначення геометричної ймовірності з курсу теорії ймовірності одержимо вираз для визначення ймовірності успіху порушника в наступному виді:

$$P_{под} = \frac{T_{оп} - t_{под}}{T_{оп}} = 1 - \frac{t_{под}}{T_{оп}}. \qquad (15.6)$$

Тоді ймовірність виявлення несанкціонованих дій порушника буде визначатися виразами:

$$P_в = 1 - P_{под}, \qquad (15.7)$$

$$P_в = \frac{t_{под}}{T_{оп}}. \qquad (15.8)$$

При $t_{под} > T_{оп}$ порушник буде виявлений напевно, тобто $P_в = 1$. В другому випадку, коли $T_{оп} < t_{под} < T_{вбл}$, імовірність успіху порушника буде визначатися за аналогією з попереднім співвідношенням:

$$P_{под} = 1 - \frac{t_{под}}{T_{вбл}}. \qquad (15.9)$$

Імовірність виявлення і блокування несанкціонованих дій порушника:

$$P_{вбл} = (1 - P_{под}), \qquad (15.10)$$

$$P_{вбл} = \frac{t_{под}}{T_{вбл}}. \qquad (15.11)$$

При $t_{под} > T_{вбл}$ спроба НСД не має сенсу, тому що вона буде виявлена напевно. У цьому випадку $P_{вбл}=1$.

Таким чином, розрахунок міцності перешкоди з властивостями виявлення і блокування можна робити по формулі

$$P_{сзі}=\min\{P_{вбл},(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхj})\}, \qquad (15.12)$$

де j – число шляхів обходу цієї перешкоди.

Для більш повного представлення міцності перешкоди у виді автоматизованої системи виявлення і блокування НСД необхідно враховувати надійність її функціонування і шляхи можливого обходу її порушником.

Імовірність відмовлення системи визначається по відомій формулі

$$P_в(t) = e^{-\lambda t}, \qquad (15.13)$$

де λ – інтенсивність відмовлень групи технічних засобів, що складають систему виявлення і блокування НСД;

t – інтервал часу функціонування системи виявлення і блокування НСД.

З урахуванням можливого відмовлення системи контролю міцність перешкоди буде визначатися за формулою

$$P_{сзік}=\min\{P_{вбл}(1-P_в),(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхj})\}, \qquad (15.14)$$

де $P_{вбл}$ і $P_в$ визначаються відповідно по формулах (15.11) і (15.13);

$P_{обх}$ і кількість шляхів обходу j визначаються експертним шляхом на основі аналізу принципів побудови системи контролю і блокування НСД.

На підставі викладеного підбиваємо деякі підсумки і робимо висновок про те, що захисні перешкоди бувають двох видів: контрольовані і не контрольовані людиною. Міцність неконтрольованої перешкоди розраховується за формулою (15.3), а контрольованої – за формулою (15.14).

15.2. Оцінка моделі багатоланкового захисту інформації

Прикладом такого виду захисту може служити приміщення, у якому зберігається апаратура. Як перешкоди з різною міцністю тут можуть служити стіни, стеля, підлога, вікна і замок на дверях.

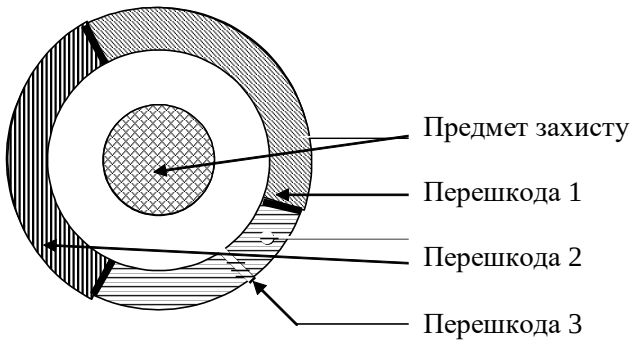

Рисунок 15.3 – Модель багатоланкового захисту

Формальний опис для міцності багатоланкового захисту практично збігається з виразами (15.2) і (15.14), тому що наявність декількох шляхів обходу однієї перешкоди, що не задовольняє заданим вимогам, зажадає їхнього перекриття відповідними перешкодами. Тоді вираз для міцності багатоланкового захисту при використанні неконтрольованих перешкод може бути представлене у виді:

$$P_{сзі}=\min\{P_{сзі1},P_{сзі2},...,P_{сзіі},(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхк})\}, \quad (15.15)$$

де $P_{сзіі}$ – міцність і-ї перешкоди.

Вираз для міцності багатоланкового захисту з контрольованими перешкодами буде в наступному виді:

$$P_{сзік}=\min\{P_{сзік1},P_{сзік2},P_{сзік3},...,P_{сзікn},(1-P_{обх1}),(1-P_{обх2}),...,(1-P_{обхj})\}, \quad (15.16)$$

де $P_{сзік}$ – міцність к-ї перешкоди.

Тут варто підкреслити, що розрахунки підсумкової міцності захисту для неконтрольованих і контрольованих перешкод повинні бути роздільними, оскільки вихідні дані для них різні, і, отже, це різні задачі, два різних контури захисту.

Якщо міцність слабкої ланки задовольняє пред'явленим вимогам контуру захисту в цілому, виникає питання про надмірність міцності на інших ланках даного контуру. Звідси випливає, що економічно доцільно застосовувати в багатоланковому контурі захисту рівні за міцністю перешкоди.

Тоді сумарна міцність дубльованих перешкод буде визначатися за формулою

$$P_{\Sigma} = 1 - \prod_{i=1}^{m}(1 - P_i), \quad (15.17)$$

де i=1,m – порядковий номер перешкоди;

P_i– міцність і-ї перешкоди.

У відповідальних випадках при підвищених вимогах до захисту застосовується багаторівневий захист, модель якого представлена на рис. 15.4.

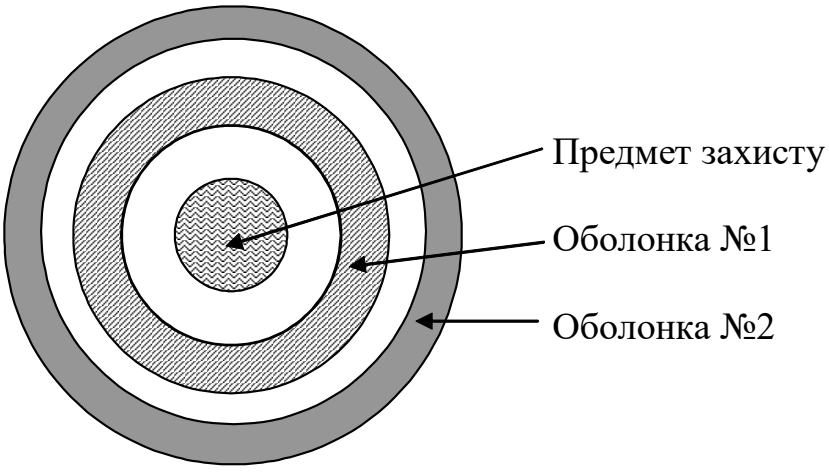

Рисунок 15.4 – Модель багаторівневого захисту

Під час розрахунку сумарної міцності декількох контурів захисту у формулу (15.17) замість P_i включається $P_{кі}$ – міцність кожного контуру, значення якої визначається по одній з формул (15.15) і (15.16), тобто для контрольованих і неконтрольованих перешкод знову розрахунки повинні бути роздільними і проводитись для різних контурів, що утворять кожний окремий багаторівневий захист. При $P_{кі} = 0$ даний контур у розрахунок не приймається. При $P_{кі.} = 1$ інші контури захисту є надлишковими. Підкреслимо також, що дана модель справедлива лише для контурів захисту, що перекривають ті самі канали несанкціонованого доступу до предмета захисту.

15.3. Методика розрахунку міцності захисту.

У табл. 15.1 не приведені засоби контролю цілісності програмного забезпечення і інформації в АС, а також засоби реєстрації, рекомендовані звичайно сучасними фахівцями і нормативними документами. Ці засоби не мають досить швидкої реакції на НСД і є необхідними лише для оцінки наслідків після того, як подія вже здійснилася, і порушник може бути вже далеко. Їхні функції захисту ефективні лише в стримуванні потенційного некваліфікованого порушника. Процедура контролю цілісності в принципі видає операторові інформацію про порушення, але тільки в момент проведення цієї процедури. Її частота проведення, як правило, встановлюється організаційно і проводиться відносно рідко через великий час процедури і відволікання значних ресурсів ЕОМ. Однак необхідність у застосуванні цих засобів не заперечується. Вони необхідні для дублювання основних засобів, але насамперед для проведення аналізу події і виявлення випадкових впливів.

Таблиця 15.1 – Розподіл засобів захисту по можливих каналах НСД

№ п/п	Найменування можливого каналу НСД	Клас захисту			Засоби захисту	Міцність
		I	II	III		
1	2	3	4	5	6	7
1	Пристрій введення (виводу) інформації	+ + + +	+ + + +	+ - + +	Система контролю і розмежування доступу в приміщення. Програмно-апаратний комплекс контролю входу в систему. Програма контролю і розмежування доступу до ПЗ й інформації АС. Антивірусні засоби.	Р1 Р2 Р3 Р4
2	Апаратура відображення і документування інформації	+	+	+	Система розмежування і контролю доступу в приміщення.	Р1
3	Апаратура, що ремонтується та знаходиться	+ +	+ +	- -	Система розмежування і контролю доступу в приміщення.	Р1 Р5

	на профілактиці				Система контролю введення (виводу) апаратури в (з) робочий контур обміну інформацією.	
		+	+	+	Засоби стирання залишків інформації.	Р14
		+	-	-	Засоби накладення на залишки інформації випадкової послідовності символів і чисел.	Р15 Р16
		+	-	-	Засоби знищення носіїв секретної інформації.	
4	Машинні носії інформації	+	+	+	Облік і розмежування доступу до носіїв.	Р6
		+	-	-	Електронна ідентифікація носіїв.	Р7
		+	-	-	Шифрування інформації. Резервування інформації з	Р8
		+	+	-	охороною її копії.	Р9
5	Документи	+	+	+	Облік, реєстрація і розмежування доступу до документів.	Р10
6	Носії програмного забезпечення	+	+	+	Облік, реєстрація і розмежу-вання доступу до носіїв ПЗ.	Р11
		+	+	+	Верифікація і контроль цілісності ПЗ.	Р12
		+	+	+	Резервування ПЗ з контролем доступу до його копії.	Р13
7	Машинні носії з залишками інформації (диски, стрічки)	+	+	+	Облік, реєстрація і розмежування доступу.	Р6
		+	+	+	Засоби стирання інформації.	Р14
		+	-	-	Накладення випадкової послідовності символів і чисел.	Р15
		+	-	-	Засоби знищення носіїв.	Р16
8	Паперові носії з залишками інформації	+	+	-	Засоби знищення носіїв.	Р17
9	Засоби завантаження ПЗ	+	+	+	Засоби контролю і розмежування доступу в приміщення.	Р1
		+	+	-	Засоби контролю і блокування доступу до завантаження ПЗ.	Р18
		+	+	+	Антивірусні засоби.	Р4
10	Пульти й органи керування, внутрішній монтаж апаратури	+	+	-	Засоби контролю і розмежування доступу в приміщення.	Р1
		+	+	-	Система контролю розкриття апаратури.	Р19

11	Внутрішні лінії зв'язку між апаратними засобами АС	+ + - +	+ + + -	- - - -	Засоби контролю доступу на територію АС. Засоби контролю розкриття апаратури. Схована прокладка ліній зв'язку. Шифрування переданої інформації.	Р1 Р19 Р20 Р21
12	Зовнішні канали зв'язку АС	+ + +	+ - +	+ - +	Програма контролю і розмежування доступу до інформації АС (на вході АС). Шифрування інформації, що передається. Антивірусі засоби	Р24 Р22
13	Побічне Електромагніт-не випромі нювання і наведення інформації	+	-	-	Засоби зниження або зашум-лення рівня випромінювання і наведень інформації на границі контрольованої зони об'єкта АС.	Р23
14	Сміттєвий кошик	+	+	-	Засоби знищення носіїв закритої інформації.	Р17
Примітка: Знак "+" - наявність засобу захисту; знак "-" - відсутність засобу захисту.						

Для розрахунку міцності захисту інформації в АС проводиться аналіз можливого каналу НСД на предмет відповідності їхнього складу і кількості заданому класу захисту, поділу їх на контрольовані і неконтрольовані, наявність відповідних засобів захисту і можливе їхнє дублювання. До контрольованого в нашому прикладі по I класу захисту пропонується віднести засоби зі значеннями міцності: Р1, Р2, Р3, Р5, Р6, Р10, Р11, Р18, Р19, Р24.

Перераховані значення обчислюються за формулою (15.14).

Для кожного можливого каналу НСД з урахуванням дублювання засобів захисту обчислюється значення міцності захисту. У нашому випадку такий розрахунок для каналів NN1, 3, 9, 10, 11 виробляється за формулою (15.17).

Після порівняння отриманих значень вибираємо менше з них, що і буде значенням міцності захисної оболонки, утвореної даними засобами, тобто використовуємо формулу (15.16).

До неконтрольованого можна віднести засоби з наступними значеннями міцності: Р8, Р14, Р15, Р16, Р17, Р21, Р23.

Розрахунок міцності захисту для кожного каналу ведемо аналогічним способом, використовуючи відповідні формули (15.1), (15.2), (15.12), оболонки в цілому - за формулами (15.10), (15.15) (15.16).

Чим більша довжина пароля, тим більшу безпеку буде забезпечувати система, тому що будуть потрібні великі зусилля для відгадування пароля. Цю

обставину можна представити в термінах очікуваного часу розкриття пароля, або очікуваного безпечного часу. Очікуваний безпечний час – напівдобуток числа можливих паролів і часу, необхідного для того, щоб спробувати кожен пароль з послідовності запитів, тобто

$$t_{БЧ} = \frac{N_{ПАР} \cdot t_{ПАР}}{2} = \frac{N_{ПАР} \cdot N_{СИМ}}{2 \cdot R}, \quad N_{ПАР} = A^S, \tag{15.18}$$

де R - швидкість передачі (у симв/хв) у лінії зв'язку;

$N_{СИМ}$ - кількість символів у кожному переданому повідомленні при спробі одержати доступ (включаючи пароль і службові сим-воли);

$N_{ПАР}$ – кількість всіляких паролів;

$t_{ПАР}$ – час, необхідний для того, щоб спробувати кожен пароль з послідовності запитів;

S - довжина пароля;

A - число символів в алфавіті, з якого складається пароль (тобто для англійського A=26).

Приклад. Якщо R=60 млн. симв/хв, $N_{СИМ}$=20, S=8 і A=26, то безпечний час, що очікується,

$$t_{БЧ} = \frac{N_{ПАР} \cdot N_{СИМ}}{2 \cdot R} = \frac{A^S N_{СИМ}}{2 \cdot R} = \frac{26^8 \cdot 20}{2 \cdot 60 \cdot 10^6} = 34804{,}511 \text{ хв} \approx 24{,}2 \text{ доби}.$$

Якщо після кожної невдалої спроби автоматично передбачається десятисекундна затримка, то цим самим очікуваний час, необхідний для розкриття пароля, збільшується в шість разів і стає рівним приблизно шістдесяти рокам.

Якщо на додаток до R, $N_{СИМ}$, $N_{ПАР}$, S і A, визначеним вище, приймемо, що P - ймовірність того, що відповідний пароль може бути розкритий сторонньою особою, і $t_{ВІДКР.ПАР}$ - період часу, протягом якого можуть бути здійснені систематичні спроби, то P має нижню границю P_O, де

$$P_O = \frac{N_{ВІДКР.ПАР}}{N_{ПАР}}, \tag{15.19}$$

де $N_{ВІДКР.ПАР}$ - кількість спроб відкриття пароля за час $t_{ВІДКР.ПАР}$, дорівнює

$$N_{ВІДКР.ПАР} = \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ}}.$$

Тоді (15.2) можна представити у виді:

$$P_O = \frac{N_{ВІДКР.ПАР}}{N_{ПАР}} = \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ} N_{ПАР}} = \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ} A^S}, \tag{15.20}$$

оскільки $P \geq P_O$, то

$$P \geq \frac{R \cdot t_{ВІДКР.ПАР}}{N_{СИМ} A^S}. \tag{15.21}$$

Переписавши (15.21) інакше, отримаємо формулу Андерсена

$$A^S \geq \frac{R \cdot t_{ВІДКР.ПАР}}{P \cdot N_{СИМ}}. \qquad (15.22)$$

Якщо R, $N_{СИМ}$, $t_{ВІДКР.ПАР}$ і A фіксовані, то кожне значення S (довжина пароля) буде давати різну ймовірність P правильного його відгадування. Тоді для побудуви системи, де незаконний користувач мав би ймовірність відгадування правильного пароля не більшу, ніж P, варто вибрати таке S, що задовольняє виразу (15.22).

Приклад. Припустимо, що ми хочемо, використовуючи стандартний англійський шрифт, встановити такий пароль, щоб ймовірність його відгадування була не більшою 1/1000 (0,001) після тримісячного систематичного тестування. Припустимо, що швидкість передачі по лінії зв'язку $60 \cdot 10^6$ симв/хв і що за одну спробу посилається 20 символів. Використовуючи співвідношення (5.22), отримуємо

$$26^S \geq \frac{60 \cdot 10^6 \cdot 3 \cdot 30 \cdot 24 \cdot 60}{20 \cdot 0{,}001} = 3{,}888 \cdot 10^{15}.$$

Для S=6 отримаємо $26^S=3{,}089 \cdot 10^8$, і для S=7 – $26^7=8{,}03 \cdot 10^9$. Отже, за даних обставин нам варто вибрати S=7.

Як бачимо, на ймовірність P розкриття пароля робить вплив величина S. Збільшення довжини пароля тільки на один символ значно збільшує час, необхідний зловмисникові для розкриття цього пароля при систематичних спробах, організованих за допомогою ЕОМ. Так, якщо при відповідних умовах очікуваний безпечний час для семисимвольного пароля, обраного з 36-символьного алфавіту, складе близько 9 діб, очікуваний безпечний час для восьмисимвольного пароля складе 11 місяців.

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

1. Провести оцінку моделей систем захисту інформації.

1.1. Визначити імовірність неподолання перешкоди порушником $P_{сзі}$, при $P_{обх}=0$ і $t_ж > t_{под}$, користуючись даними таблиці. Зробити висновки.

Таблиця 15.2 – Вихідні дані для розрахунку

№ варіанту	$P_{под}$
1.	0,25
2.	0,28
3.	0,25
4.	0,28
5.	0,31
6.	0,34
7.	0,37
8.	0,4
9.	0,43
10.	0,46
11.	0,49
12.	0,52
13.	0,55
14.	0,58
15.	0,61
16.	0,64
17.	0,67
18.	0,7
19.	0,73
20.	0,76

21.	0,79
22.	0,82
23.	0,85
24.	0,88
25.	0,91

26.	0,94
27.	0,97
28.	1
29.	1,03
30.	1,06

1.2. Провести розрахунок $P_{сзі}$ по формулі 15.2, відповідно до варіанту та даних таблиці 15.3. Зробити висновки.

Таблиця 15.3 – Вихідні дані для розрахунку

№ варіанту	$P_{под}$	$P_{обх}$
2.	0,83	0,44
3.	0,89	0,97
4.	0,43	0,5
5.	0,13	0,69
6.	0,98	0,26
7.	0,75	0,83
8.	0,13	0,78
9.	0,64	0,42
10.	0,14	0,25
11.	0,55	0,43
12.	0,04	0,33
13.	0,18	0,92
14.	0,89	0,23
15.	0,01	0,17
16.	0,9	0,75
17.	0,63	0,14
18.	0,22	0,35
19.	0,06	0,11
20.	0,23	0,47
21.	0,89	0,62
22.	0,49	0,76
23.	0,94	0,57
24.	0,19	0,13
25.	0,59	0,26
26.	0,19	0,96
27.	0,73	0,72
28.	0,53	0,52
29.	0,63	0,44
30.	0,82	0,97

1.3. Провести розрахунок $P_{сзі}$ по формулі 15.3, відповідно до варіанту та даних таблиці 15.4.

Таблиця 15.4 – Вихідні дані для розрахунку

№ варіанту	$P_{под}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$	$P_{обх4}$	$P_{обх5}$
1.	0,74	0,81	0,33	0,82	0,15	0,16
2.	0,74	0,44	0,18	0,77	0,92	0,16
3.	0,48	0,7	0,29	0,92	0,76	0,13
4.	0,61	0,57	0,99	0,62	0,43	0,79
5.	0,67	0,55	0,28	0,49	0,28	0,08
6.	0,42	0,57	0,92	0,68	0,47	0,85
7.	0,64	0,21	0,85	0,73	0,28	0,38
8.	0,91	0,71	0,95	0,17	0,8	0,95
9.	0,39	0,97	0,57	0,35	0,23	0,48
10.	0,71	0,97	0,92	0,43	0,53	0,03
11.	0,84	0,06	0,23	0,35	0,94	0,5
12.	0,11	0,36	0,31	0,05	0,83	0,87
13.	0,6	0,81	0,85	0,47	0,61	0,67

14.	0,05	0,61	0,93	0,25	0,36	0,53
15.	0,86	0,52	0,15	0,83	0,42	0,93
16.	0,02	0,59	0,05	0,62	0,38	0,46
17.	0,89	0,2	0,83	0,99	0,76	0,49
18.	0,15	0,01	0,03	0,61	0,28	0,99
19.	0,11	0,24	0,71	0,97	0,3	0,3
20.	0,33	0,29	0,93	0,71	0,63	0,25
21.	0,07	0,59	0,57	0,37	0,23	0,13
22.	0,15	0,18	0,61	0,64	0,66	0,16
23.	0,21	0,99	0,14	0,62	0,45	0,83
24.	0,55	0,03	0,72	0,89	0,82	0,13
25.	0,8	0,99	0,47	0,84	0,93	0,57
26.	0,96	0,81	0,11	0,81	0,5	0,73
27.	0,02	0,21	0,4	0,77	0,23	0,76
28.	0,29	0,62	0,61	0,69	0,92	0,63
29.	0,23	0,57	0,61	0,95	0,32	0,48
30.	0,2	0,4	0,89	0,06	0,52	0,16

1.4.Провести підбір параметрів $T_{оп}$, $t_{спр}$, $t_{в}$, $t_{бл}$, при $t_{под}$=0,7 для задоволення умови (15.4) або (15.5).

1.5.Провести підбір параметрів $T_{оп}$, $t_{под}$, щоб $P_{под}$=X відповідно до формули (15.6). X вибирається з таблиці 15.5 відповідно до варіанту:

Таблиця 15.5.

№ варіанту	X
1.	0,1
2.	0,15
3.	0,25
4.	0,2
5.	0,18
6.	0,21
7.	0,23
8.	0,16
9.	0,22
10.	0,27
11.	0,3
12.	0,31
13.	0,32
14.	0,33
15.	0,34
16.	0,35
17.	0,36
18.	0,37
19.	0,38
20.	0,39
21.	0,12
22.	0,13
23.	0,14
24.	0,17
25.	0,19
26.	0,11
27.	0,4
28.	0,41
29.	0,42
30.	0,43

1.6. Провести розрахунок $P_{сзі}$ по формулі 15.3, відповідно до варіанту та даних таблиці 15.6.

Таблиця 15.6 – Вихідні дані для розрахунку

№ варіанту	$t_{под}$, с	$T_{оп}$ с	$t_{спр}$ с	$t_{в}$ с	$t_{бл}$ с	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
1.	130	82	25	35	15	0,17	0,25	0,45
2.	131	81	26	34	16	0,81	0,54	0,48
3.	132	80	27	33	17	0,43	0,39	0,64
4.	133	79	28	32	18	0,83	0,17	0,7
5.	134	78	29	31	19	0,49	0,07	0,53
6.	135	77	30	30	20	0,24	0,63	0,09
7.	136	76	31	29	21	0,62	0,46	0,73
8.	137	75	32	28	22	0,73	0,01	0,51
9.	138	74	33	27	23	0,49	0,14	0,11
10.	139	73	34	26	24	0,62	0,98	0,15
11.	140	72	35	25	25	0,63	0,34	0,91
12.	141	71	36	24	26	0,52	0,44	0,36
13.	142	70	37	23	27	0,49	0,63	0,57
14.	143	69	38	22	28	0,91	0,38	0,26
15.	144	68	39	21	29	0,02	0,26	0,63
16.	145	67	40	20	30	0,94	0,43	0,49
17.	146	66	41	19	31	0,29	0,75	0,04
18.	147	65	42	18	32	1	0,65	0,8
19.	148	64	43	17	33	0,03	0,14	0,71
20.	149	63	44	16	34	0,61	0,77	0,43
21.	150	62	45	15	35	0,15	0,68	0,76
22.	151	61	46	14	36	0,16	0,17	0,97
23.	152	60	47	13	37	0,54	0,52	0,79
24.	153	59	48	12	38	0,27	0,96	0,82
25.	154	58	49	11	39	0,72	0,25	0,41
26.	155	57	50	10	40	0,53	0,13	0,54
27.	156	56	51	9	41	0,29	0,34	0,11
28.	157	55	52	8	42	0,76	0,82	0,7
29.	158	54	53	7	43	0,41	0,38	0,18
30.	159	53	54	6	44	0,23	0,65	0,69

1.7. Підібрати параметри λ , t , імовірність відмовлення системи відповідно до формули (15.13) складала 0,05.

2. Провести оцінку моделі багатоланкового захисту.

2.1. Розрахувати міцність захисту при використанні неконтрольованих перешкод відповідно до формули (15.15) при наступних параметрах, таблиця 15.7.

Таблиця 15.7.

№ варіанту	$P_{сзі1}$	$P_{сзі2}$	$P_{сзі3}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
1.	0,04	0,99	0,64	0,75	0,57	0,09

2.	0,09	0,91	0,07	0,74	0,73	0,85
3.	0,25	0,62	0,28	0,03	0,38	0,77
4.	0,52	0,4	0,53	0,21	0,73	0,79
5.	0,21	0,45	0,27	0,89	0,26	0,92
6.	0,52	0,83	0,63	0,35	0,6	0,16
7.	0,71	0,78	0,59	0,32	0,3	0,8
8.	0,81	0,46	0,96	0,75	0,27	0,51
9.	0,93	0,35	0,41	0,94	0,77	0,23
10.	0,54	0,65	0,26	0,5	0,44	0,04
11.	0,22	0,96	0,56	0,58	0,01	0,29
12.	0,65	0,3	0,74	0,36	0,87	0,99
13.	0,29	0,07	0,82	0,05	0,46	0,44
14.	0,51	0,86	0,41	0,32	0,16	0,9
15.	0,23	0,17	0,74	0,04	0,82	0,06
16.	0,78	0,5	0,96	0,98	0,59	0,87
17.	0,18	0,57	0,86	0,51	0,58	0,49
18.	0,43	0,05	0,23	0,86	0,66	0,44
19.	0,2	0,18	0,98	0,81	0,07	0,68
20.	0,14	0,77	0,83	0,43	0,61	0,34
21.	0,47	0,83	0,28	0,65	0,88	0,52
22.	0,09	0,18	0,3	0,01	0,42	0,75
23.	0,02	0,86	0,64	0,75	0,94	0,14
24.	0,55	0,42	0,93	0,74	0,03	0,5
25.	0,03	0,54	0,08	0,03	0,92	0,47
26.	0,19	0,2	0,9	0,21	0,03	0,53
27.	0,13	0,88	0,4	0,89	0,84	0,55
28.	0,42	0,63	0,36	0,35	0,62	0,96
29.	0,77	0,42	0,2	0,32	0,56	0,51
30.	0,53	0,65	0,61	0,75	0,17	0,02

2.2. Провести розрахунок міцності багатоланкового захисту з контрольованими перешкодами відповідно до формули 15.16 при наступних параметрах, таблиця 15.8.

Таблиця 15.8

№ варіанту	$P_{сзі1}$	$P_{сзі2}$	$P_{сзі3}$	$P_{обх1}$	$P_{обх2}$	$P_{обх3}$
1.	0,02	0,84	0,62	0,17	0,28	0,33
2.	0,37	0,87	0,02	0,08	0,36	0,1
3.	0,4	0,87	0,82	0,47	0,94	0,23
4.	0,41	0,19	0,29	0,94	0,61	0,26
5.	0,26	0,67	0,73	0,37	0,58	0,28
6.	0,33	0,68	0,18	0,89	0,15	0,9
7.	0,86	0,21	0,04	0,59	0,76	0,98
8.	0,6	0,78	0,11	0,77	0,07	0,02

9.	0,76	0,06	0,61	0,29	0,4	0,49
10.	0,49	0,99	0,51	0,35	0,07	0,62
11.	0,21	0,03	0,18	0,19	0,76	0,02
12.	0,56	0,92	0,58	0,52	0,57	0,6
13.	0,2	0,48	0,17	0,39	0,1	0,31
14.	0,6	0,03	0,27	0,64	0,06	0,48
15.	0,72	0,17	0,82	0,02	0,92	0,25
16.	0,43	0,89	0,36	0,39	0,48	0,08
17.	0,79	0,41	0,64	0,99	0,9	0,87
18.	0,71	0,25	0,35	0,94	0,89	0,96
19.	0,01	0,39	0,74	0,36	0,55	0,96
20.	0,94	0,52	0,8	0,65	0,19	0,9
21.	0,39	0,6	0,06	0,84	0,96	0,98
22.	0,28	0,4	0,38	0,8	0,77	0,89
23.	0,43	0,08	0,01	0,17	0,88	0,04
24.	0,79	0,35	0,62	0,12	0,05	0,28
25.	0,51	0,46	0,18	0,39	0,99	0,9
26.	0,19	0,71	0,1	0,53	0,98	0,01
27.	0,97	0,94	0,87	0,12	0,45	0,27
28.	0,99	0,91	0,56	0,76	0,29	0,5
29.	0,69	0,46	0,67	0,65	0,2	0,28
30.	0,1	0,94	0,29	0,7	0,28	0,76

2.3. Провести розрахунок сумарної міцності.

3. Провести розрахунок міцності захисту.

Провести розрахунок міцності контрольованого по І класу захисту інформації при наступних параметрах, таблиця 15.9:

Таблиця 15.9

№ варіанту	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
1.	0,02	0,84	0,62	0,17	0,28	0,33	0,03	0,5	0,4	0,08	0,09	0,1
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,37	0,87	0,02	0,08	0,36	0,1	0,4	0,87	0,82	0,47	0,94	0,23
2.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,37	0,87	0,02	0,08	0,36	0,1	0,02	0,84	0,62	0,17	0,28	0,33
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,02	0,84	0,62	0,17	0,28	0,33	0,03	0,5	0,4	0,08	0,09	0,1
3.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,4	0,87	0,82	0,47	0,94	0,23	0,03	0,5	0,4	0,08	0,09	0,1
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,41	0,19	0,29	0,94	0,61	0,26	0,26	0,67	0,73	0,37	0,58	0,28
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
4.	0,26	0,67	0,73	0,37	0,58	0,28	0,26	0,26	0,67	0,73	0,37	0,58
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}

	0,33	0,68	0,18	0,89	0,15	0,9	0,26	0,26	0,67	0,73	0,37	0,58
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
5.	0,86	0,21	0,04	0,59	0,76	0,98	0,26	0,26	0,67	0,73	0,37	0,58
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,6	0,78	0,11	0,77	0,07	0,02	0,49	0,99	0,51	0,35	0,07	0,62
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
6.	0,76	0,06	0,61	0,29	0,4	0,49	0,56	0,92	0,58	0,52	0,57	0,6
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,49	0,99	0,51	0,35	0,07	0,62	0,6	0,03	0,27	0,64	0,06	0,48
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
7.	0,21	0,03	0,18	0,19	0,76	0,02	0,43	0,89	0,36	0,39	0,48	0,08
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,56	0,92	0,58	0,52	0,57	0,6	0,86	0,21	0,04	0,59	0,76	0,98
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
8.	0,2	0,48	0,17	0,39	0,1	0,31	0,6	0,78	0,11	0,77	0,07	0,02
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,6	0,03	0,27	0,64	0,06	0,48	0,76	0,06	0,61	0,29	0,4	0,49
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
9.	0,72	0,17	0,82	0,02	0,92	0,25	0,21	0,03	0,18	0,19	0,76	0,02
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,43	0,89	0,36	0,39	0,48	0,08	0,2	0,48	0,17	0,39	0,1	0,31
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,79	0,41	0,64	0,99	0,9	0,87	0,49	0,99	0,51	0,35	0,07	0,62
10.	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,71	0,25	0,35	0,94	0,89	0,96	0,43	0,89	0,36	0,39	0,48	0,08
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
11.	0,01	0,39	0,74	0,36	0,55	0,96	0,6	0,03	0,27	0,64	0,06	0,48
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,94	0,52	0,8	0,65	0,19	0,9	0,72	0,17	0,82	0,02	0,92	0,25
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,39	0,6	0,06	0,84	0,96	0,98	0,6	0,03	0,27	0,64	0,06	0,48
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,28	0,4	0,38	0,8	0,77	0,89	0,33	0,68	0,18	0,89	0,15	0,9
12.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,43	0,08	0,01	0,17	0,88	0,04	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,79	0,35	0,62	0,12	0,05	0,28	0,33	0,68	0,18	0,89	0,15	0,9
13.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,51	0,46	0,18	0,39	0,99	0,9	0,6	0,03	0,27	0,64	0,06	0,48
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,19	0,71	0,1	0,53	0,98	0,01	0,2	0,48	0,17	0,39	0,1	0,31
14.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25

	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,99	0,91	0,56	0,76	0,29	0,5	0,6	0,03	0,27	0,64	0,06	0,48
15.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,69	0,46	0,67	0,65	0,2	0,28	0,33	0,68	0,18	0,89	0,15	0,9
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,1	0,94	0,29	0,7	0,28	0,76	0,2	0,48	0,17	0,39	0,1	0,31
16.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,03	0,5	0,4	0,08	0,09	0,1	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,03	0,5	0,4	0,08	0,09	0,1	0,33	0,68	0,18	0,89	0,15	0,9
17.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,03	0,5	0,4	0,08	0,09	0,1	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
18.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
							0,33	0,68	0,18	0,89	0,15	0,9
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,97	0,94	0,87	0,12	0,45	0,27
19.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,26	0,26	0,67	0,73	0,37	0,58	0,2	0,48	0,17	0,39	0,1	0,31
20.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,33	0,68	0,18	0,89	0,15	0,9
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,97	0,94	0,87	0,12	0,45	0,27
21.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
							0,72	0,17	0,82	0,02	0,92	0,25
22.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,97	0,94	0,87	0,12	0,45	0,27	0,33	0,68	0,18	0,89	0,15	0,9
23.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,2	0,48	0,17	0,39	0,1	0,31	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,33	0,68	0,18	0,89	0,15	0,9	0,97	0,94	0,87	0,12	0,45	0,27
24.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,33	0,68	0,18	0,89	0,15	0,9
25.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}

	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
26.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,33	0,68	0,18	0,89	0,15	0,9
27.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,26	0,26	0,67	0,73	0,37	0,58	0,72	0,17	0,82	0,02	0,92	0,25
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,97	0,94	0,87	0,12	0,45	0,27	0,2	0,48	0,17	0,39	0,1	0,31
28.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,33	0,68	0,18	0,89	0,15	0,9	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,2	0,48	0,17	0,39	0,1	0,31	0,33	0,68	0,18	0,89	0,15	0,9
29.	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}
	0,26	0,26	0,67	0,73	0,37	0,58	0,97	0,94	0,87	0,12	0,45	0,27
	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}
	0,97	0,94	0,87	0,12	0,45	0,27	0,72	0,17	0,82	0,02	0,92	0,25

4. Провести оцінку довжини паролів і безпечного часу їх використання. Використовуючи англійський шрифт та клавіші CapsLock, Shift, та цифрові клавіші встановити таку довжину, щоб ймовірність його відгадування була не більшою 1/1000 (0,001) після тримісячного систематичного тестування. Припустимо, що швидкість передачі по лінії зв'язку $50 \cdot 10^6$ симв/хв і що за одну спробу посилається 25 символів.

5. Зробити висновки та оформити звіт.

ЗМІСТ ЗВІТУ

1. Назва, мета заняття.
2. Опис дій в ході виконання роботи підтверджений відповідними розрахунками.
3. Висновки про виконану роботу.