Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Организация и обеспечение аудита настроек средств защиты информации»

ОТЧЕТ ПО МОДУЛЮ №2

«Organization of IS»

Выполнил:

Чу Ван Доан, студент группы N3347

(подпись)

Проверил:

Пенин Андрей Семенович

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

Содержание

Содержание.. 2
Введение.. 4
Задание.. 5
Ход работы.. 6
1. Analyze the company, identify the main information security problems, and identify the main risks.. 6
1.1. Description of the company's main activity.. 6
1.2. Analysis of infrastructure and security processes.. 6
1.3. List of major risks and potential consequences.. 7
2. Assess the risks, identify those that can be ignored.. 8
3. Develop an Information Security (IS) Plan.. 9
3.1. Information Security Policy.. 9
3.2. Technical Security Measures.. 9
3.3. Organizational Security Measures.. 9
3.4. Incident Response Plan.. 10
Заключение.. 11

Введение

Module Objective:

Analyze and develop an information security plan for the company based on the provided case. This module will guide the assessment of the company's current infrastructure and security processes, identify key risks, classify their severity, and formulate a comprehensive security plan. The plan will include security policies, technical measures, organizational measures, and incident response procedures.

Задание

10 . Retailsky JSC

Is a retail brand that sells electronics through physical stores and online. Customer data is being processed: Full name, contact information, purchase information, warranty service. The annual turnover is about 1 billion rubles, more than 50,000 customers.

1. Analyze the company, identify the main information security problems, and identify the main risks (up to 4 points)

- Describe the main activity of the company.
- Analyze the company's existing infrastructure and processes in the context of security. (Here you should, by and large, indicate the number of APMs, which ICS and ISPs may be in the company, and the installed security software. Use common sense from the point of view that a small sole proprietor for 300 clients is unlikely to have any incredible SPI built, where the ITU alone costs under a million rubles.)
- Specify the key information security issues that may threaten the company's assets.
- Formulate a list of the main risks (with a specific description of the possible consequences).

2. Assess the risks, identify those that can be ignored (up to 3 points)

- Classify the risks according to the levels of criticality (high, medium, low).
- Determine which of the risks require immediate response, and which can be left unchanged, describing the reason for making such a decision (for example, a low probability of implementation).

3. Develop a IS plan (up to 3 points)

- Formulate an information security policy.
- Prepare a set of technical measures to protect information (for example, the use of firewalls, antivirus software, encryption).
- Create a set of organizational information security measures (for example, employee training, access control, audit).
- Develop a set of responses to information security incidents (description of the incident handling process, ways to restore systems).

Ход работы

1. Analyze the company, identify the main information security problems, and identify the main risks

Сотрудник получил письмо, якобы от имени банка, с просьбой перейти по ссылке и ввести учетные данные. После выполнения действий злоумышленники получили доступ к внутренним системам компании.

1.1. Description of the company's main activity

Retailsky JSC is a retail brand specializing in selling electronic devices through both physical stores and an online platform. The company processes a large amount of customer data, including:

- Full name
- Contact information (phone number, email)
- Purchase information (products, purchase history)
- Warranty service (maintenance requests, repair history)

The company has more than 50,000 customers, with an annual revenue of approximately 1 billion rubles.

1.2. Analysis of infrastructure and security processes

Technology infrastructure:

- Online sales platform (e-commerce system).
- Customer Relationship Management (CRM) system.
- Online payment system (Payment Gateway).
- Databases storing customer information, orders, and warranties.
- Data storage and backup systems.
- Identity and Access Management (IAM) system.

Potential security issues:

- Cyberattacks: Retailsky JSC’s e-commerce platform is a potential target for cybercriminals through attacks such as DDoS, SQL Injection, and Phishing.

- Customer data breaches: If security measures are inadequate, sensitive customer data may be leaked.
- Fraudulent transactions: Hackers can exploit payment system vulnerabilities to conduct fraudulent transactions or steal credit card information.
- Insider threats: Employees with access to sensitive data may intentionally or unintentionally leak customer information.
- Data loss: Due to system failures, ransomware attacks, or backup errors.

1.3. List of major risks and potential consequences

Risk	Description	Potential Consequences
DDoS Attack	Hackers launch denial-of-service attacks, disrupting website operations.	Website downtime, revenue loss, reputation damage.
Customer Data Breach	Customer data is stolen due to security vulnerabilities or insider threats.	Loss of customer trust, legal penalties under data protection laws.
SQL Injection	Hackers exploit vulnerabilities to gain unauthorized access to databases.	Data theft, unauthorized changes to company records.
Fraudulent Transactions	Exploiting payment system weaknesses to commit fraud.	Financial loss, loss of control over transactions.
Ransomware Attack	Malware encrypts company data, demanding a ransom for decryption.	Loss of critical data, operational downtime.
Insider Threats	Employees leak or misuse customer information.	Reputation damage, regulatory violations.

2. Assess the risks, identify those that can be ignored

Risk	Severity Level	Requires Immediate Action?	Reason
DDoS Attack	High	Yes	Directly impacts business operations.
Customer Data Breach	High	Yes	Can cause significant financial and reputational damage.
SQL Injection	High	Yes	Severe risk of database exploitation.
Fraudulent Transactions	Medium	Requires Monitoring	Can be mitigated through fraud detection systems.
Ransomware Attack	High	Yes	Can lead to complete data loss.
Insider Threats	Medium	Needs Control Measures	Requires better internal security policies.

→ Prioritized risks for immediate action: DDoS attacks, customer data breaches, SQL Injection, and ransomware attacks.

3. Develop an Information Security (IS) Plan

3.1. Information Security Policy

- Implement data protection policies aligned with **GDPR** and **PCI-DSS** (Payment Card Industry Data Security Standard).
- Require all employees to comply with internal security policies.
- Restrict access to sensitive data based on employee roles.

3.2. Technical Security Measures

Website Protection:

- Deploy Web Application Firewall (WAF) to prevent SQL Injection and Cross-Site Scripting (XSS).
- Use CDN services to mitigate DDoS attacks.

Data Encryption:

- Encrypt sensitive data using AES-256.
- Secure data transmission with SSL/TLS.

Payment Security:

- Implement 3D Secure authentication for credit card transactions.
- Use AI-powered fraud detection systems.

System Protection:

- Regularly update software and apply security patches.
- Implement strict security configurations on servers.

3.3. Organizational Security Measures

- Employee cybersecurity training.
- Regular security audits and penetration testing.
- Internal access control policies using Multi-Factor Authentication (MFA).

3.4. Incident Response Plan

- DDoS Attack: Redirect traffic through CDN, report to hosting provider.
- Customer Data Breach: Identify affected systems, notify customers, fix vulnerabilities.
- Fraudulent Transactions: Flag suspicious transactions, issue refunds if necessary.
- Ransomware Attack: Restore from backup, isolate infected systems.

Заключение

In today's digital landscape, Retailsky JSC faces significant cybersecurity threats, including DDoS attacks, data breaches, fraudulent transactions, and ransomware. Given the company’s large customer base and reliance on online sales, protecting customer data and ensuring secure transactions are critical priorities.

This Information Security Plan (IS Plan) outlines a comprehensive strategy to mitigate these risks by implementing strong technical defenses, such as firewalls, encryption, and fraud detection systems, alongside organizational measures, including employee training, access control, and regular security audits.

By prioritizing cybersecurity, Retailsky JSC can strengthen its defenses, enhance customer trust, and maintain uninterrupted business operations. Implementing this plan will ensure compliance with data protection regulations, reduce financial losses from cyber threats, and improve overall resilience against evolving security risks