МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

«МОДЕЛЬ СИСТЕМИ МЕНЕДЖМЕНТУ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ »

Автор: студентка 531 групи І. І. Кірик

Науковий керівник: к.т.н., доцент С. О. Гнатюк

АКТУАЛЬНІСТЬ

Сьогодні кіберзлочинність набуває глобального характеру і потребує об'єднаних дій для боротьби з нею. Для захисту від кібератак кожна компанія намагається застосовувати найбільш ефективні та продуктивні системи і моделі захисту інформаційних ресурсів та управління їх безпекою. Основним завданням систем управління, які, серед іншого, забезпечують цілісність даних в організації, є своєчасне та оперативне реагування на кібератаки (кіберзагрози) в інформаційно-комунікаційних системах (ІКС), виявлення та уникнення рецидиву інцидентів, визначення шляхів усунення їх наслідків і розробка превентивних заходів. Як показав аналіз, універсальної системи, яка б задовольняла усім вимогам керівників, враховувала б специфіку ІКС і забезпечувала її безперервну роботу, не існує.

Тому, надзвичайно актуальним є розробка системи NAU SD (Service Desk), який буде адаптований до вимог вищого навчального закладу та особливостей загроз безпеці його ІКС.

МЕТА ЗА ЗАВДАННЯ

Метою роботи *є підвищення рівня захищеності інформаційно-комунікаційної системи організації, за рахунок розробки системи NAU SD. Розробка такої системи також дозволить покращити якість обслуговування користувачів шляхом автоматизації роботи служби технічної підтримки.*

Для досягнення поставленої мети необхідно вирішити наступні ***завдання***:

- проаналізувати діючі міжнародні стандарти та рекомендовані практики у галузі управління інцидентами інформаційної безпеки;
- дослідити основні моделі системи менеджменту управління інцидентами інформаційної безпеки;
- розробити систему управління інцидентами інформаційної безпеки;
- провести дослідження удосконаленої системи управління інцидентами інформаційної безпеки.

Об'єкт дослідження – процес управління інцидентами інформаційної безпеки.

Предмет дослідження – методи, моделі та системи управління інцидентами інформаційної безпеки.

Апробація результатів роботи. Основні результати дипломної роботи доповідалися та обговорювалися на IV міжнародній науково-технічній конференції «ITSEC» (м. Київ, НАУ, 2014р.). Базові положення роботи опубліковано у матеріалах зазначеної конференції.

Новизна роботи полягає у тому, що розроблено систему менеджменту УІІБ, яка дозволить раціоналізувати часові та матеріально-технічні ресурси, які витрачаються на управління інцидентами; зібрати в єдиному електронному журналі усі отримані від клієнтів (працівників та студентів) заявки; сформувати електронний архів виконаних заявок; налагодити автоматичну реєстрацію заявок, які надійшли у неробочий час (при відправленні їх через веб-форму); використовувати шаблони тощо.

Практична цінність отриманих результатів полягає у тому, що запропоновано систему, яка задовольняє вимогам вищого навчального закладу і містить у собі інструментарій та функції, що необхідні для підвищення загального рівня безпеки ІКС університету.

Нормативно-правове забезпечення в галузі управління інцидентами

Аналіз нормативно-правової бази в галузі управління інцидентами інформаційної безпеки показав, що базовими є такі документи:

- **ISO/IEC 17799:2005** – «Інформаційні технології. Методи і засоби забезпечення безпеки. Збірка правил по менеджменту інформаційної безпеки»;
- **ISO/IEC 27001:2013** – «Система менеджменту інформаційної безпеки»;
- **ISO / IEC 27035:2011** – «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки»;
- **ISO/IEC TR 27035** (Information technology. Security techniques. Information security incident management) – «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки»;
- **CMU/SEI-2004-TR-015** (Defining incident management processes for CISRT) – «Визначення процесів управління інцидентами для CSIRT»;
- **NIST SP 800-61** (Computer security incident handling guide) – «Інцидент компютерної безпеки, який обробляється керівництвом».

Саме ці документи і визначають основні вимого до розробки та функціонування СУІБ.

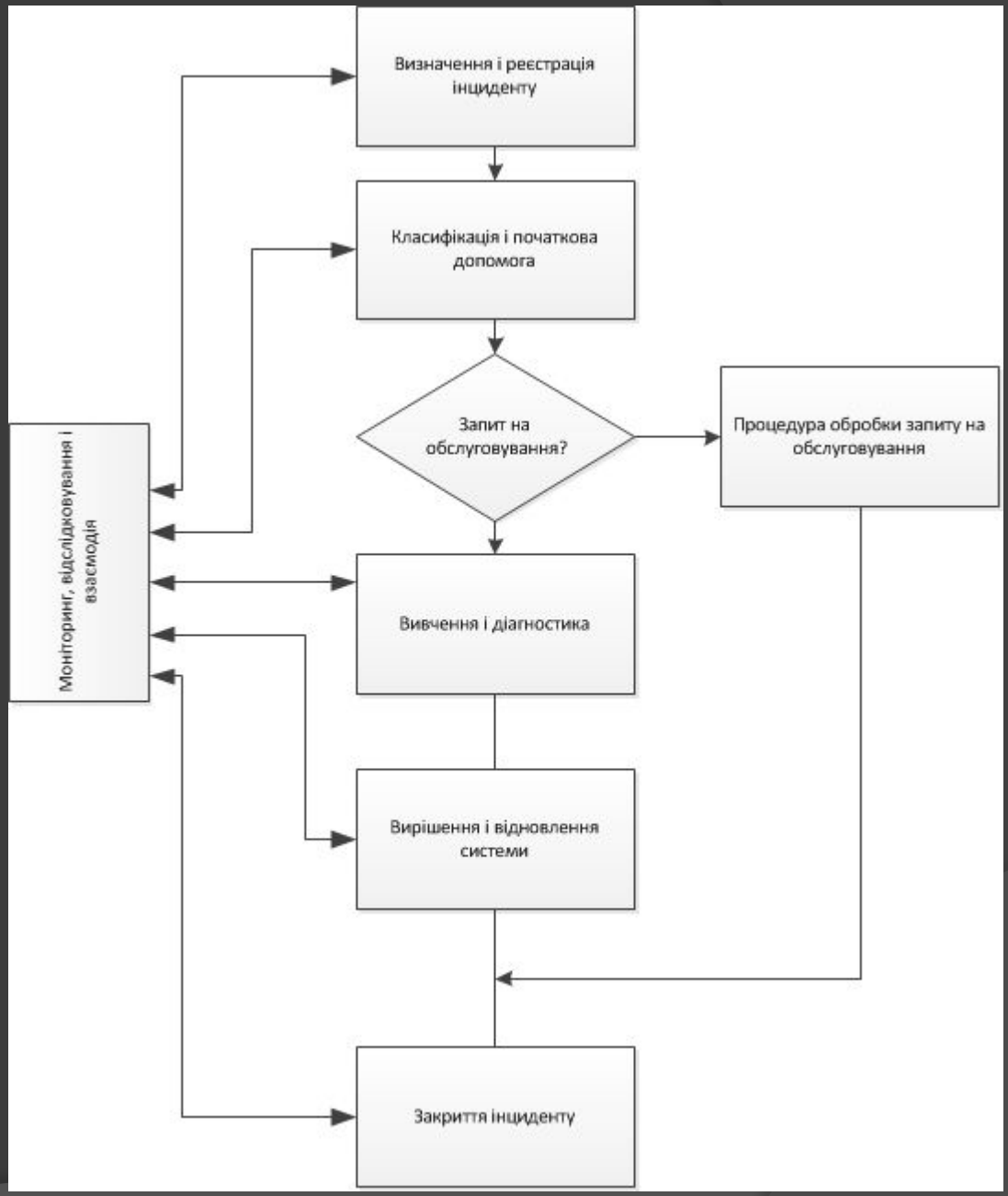
АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

№ п/п	Назва	Вартість ПЗ		Сумісність з ОС	Статистика, звіти	Моніторинг мережі	Категоризація інциденту	Журнал зміни	Надання пріоритету	Багатомовний інтерфейс	Шаблони e-mail сповіщень	Розширення для інтегрування	Моніторинг IP та мак-адреси, з якої надійшов інцидент
		демо	Ліцензова не ПЗ										
1	BPMonline Service Desk Concurrent	+	300€	-Microsoft Windows - UNIX.	+	+	+	+	+	-	-	+	-
2	OTRS IT Service Management	+	500€	Linux; - UNIX, такі як OpenBSD, FreeBSD - Windows	+	-	-	+	-	-	-	-	-
3	EnCase Enterprise	+	350€	Windows, UNIX, Linux, Solaris, Mac OS X, NetWare	+	+	+	-	+	+	-	-	-
4	nFX Log One	-	200€	Windows XP/2005 MS SQL Server 2005	+,-	-	+	-	-	-	+	-	-
5	SysAid	+	320€	Linux, UNIX,	-	-	-	+	+	+	+	-	-
6	BMC Remedy ITSM Suite 7.5	+	$850	Windows XP/2005, Linux та ін.	-	-	+	+	-	+	+	-	-
7	Axios Assyst7.5	-	$400	Windows	+	-	+	-	+	+	-	-	-
8	HP Service Manager 7.10	+	$800	Linux, UNIX, FreeBSD, Windows	-	+	+	-	+	-	-	-	-
9	Naumen Service Desk	+	$900	Windows, UNIX, Linux, Mac OS X	+	+	+	+	+	+	+	-	-

Недоліки сучасних систем

- **Висока вартість програмного продукту;**
- різні програмні платформи;
- відсутність шаблонів для подачі заявки на інцидент;
- відсутність електронного архіву виконаних заявок та ін.

СТРУКТУРА ПРОГРАМНОГО МОДУЛЯ



Висновки:

- проаналізовано діючі міжнародні стандарти та рекомендовані практики у галузі управління інцидентами інформаційної безпеки;
- досліджено основні моделі системи менеджменту управління інцидентами інформаційної безпеки;
- розроблено систему управління інцидентами інформаційної безпеки;
- проведено дослідження удосконаленої системи управління інцидентами інформаційної безпеки.

Дякую за увагу!