**Практичне заняття 3. 16.02.2021р.**

**Тема:** Аналіз існуючої єдиної автоматизованої системи документообігу структурного підрозділу Головного обчислювального центру - «ВАТ інформаційно-обчислювальний центр" – надалі ВАТ.

**Мета 1:**

1. Дати коротку характеристику комплексної системи захисту інформації (далі КСЗІ): назва підприємства, сфера діяльності, функціональні особливості; характер інформаційних ресурсів підприємства, в тому числі, які підлягають захисту.

2. Класифікувати інформацію, яку потрібно захищати.

3. Описати загрози інформаційної безпеки (види загроз, характер походження, джерела появи).

4. Описати можливі збитки, якщо можливо, оцінити в грошовому вираженні.

5. Перерахувати нормативні правові, нормативно-методичні та методичні документи, що регламентують поводження з інформацією зазначених класів.

1.1 Стисла характеристика ВАТ.

Системою захисту інформації даного підприємства є сукупність органів і/або виконавців, використовувана ними техніка захисту інформації, а також об'єкти захисту, організовані і функціонують за правилами, встановленими відповідними правовими, організаційно-розпорядчими та нормативними документами.

Місія підприємства (компанії) полягає в задоволенні ринкового попиту на перевезення, підвищення ефективності діяльності, якості послуг і глибокої інтеграції в євро-азійську транспортну систему.

Головні цілі діяльності - забезпечення потреб держави, юридичних і фізичних осіб в залізничних перевезеннях, роботах і послугах, що надаються залізничним транспортом, а також отримання прибутку.

Види діяльності, які здійснюються ВАТ:

- вантажні перевезення;

- пасажирські перевезення дальньому сполученні;

- пасажирські перевезення у приміському сполученні;

- надання послуг інфраструктури;

- надання послуг локомотивної тяги;

- ремонт рухомого складу;

- будівництво об'єктів інфраструктури;

- науково-дослідні та дослідно-конструкторські роботи;

- надання послуг соціальної сфери;

- інші види діяльності.

В організації потоком йде інформація, яка підлягає захисту – це фінансово-економічна інформація, персональні дані співробітників підприємства, інформація про експлуатаційної та виробничої діяльності, інформація про управлінську діяльність.

1.2 Класифікація інформації, що захищається.

Структурування інформації проводиться шляхом її класифікації відповідно до структури, функціями і завданнями організації з прив'язкою елементів інформації до її джерел.

В інформаційних мережах компанії відбувається циркуляція і обробка конфіденційної інформації. До неї відносяться:

- бухгалтерська інформація (заробітна плата співробітників, виплати партнерам, витрати підприємства, прибуток підприємства);

- персональні дані співробітників (бази даних співробітників, договори);

- бази даних партнерів (особиста інформація про партнерів);

- інформація про розробки;

- інформація про експлуатаційної та виробничої діяльності;

- інформація про управлінську діяльність (методи управління, план роботи).

Носіями інформації так само є і самі співробітники фірми. Таким чином, носіями інформації конфіденційного характеру є магнітні, оптичні, паперові носії: договору, звіти і інша документація.

На рис. 1 російською мовою\* наведено класифікацію інформації, що підлягає захисту.

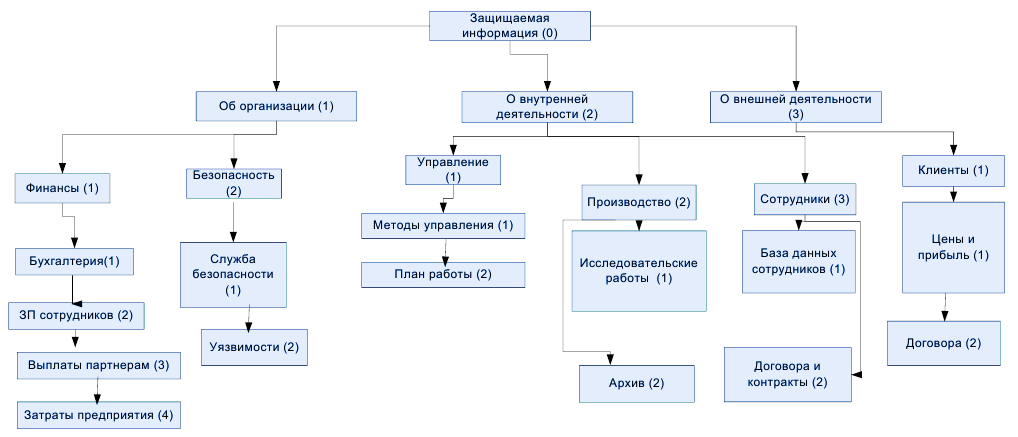


Рис.1. Граф-структура інформації, яка підлягає захисту.

1.3 Аналіз загроз.

1.3.1 Загрози інформаційної безпеці.

1. Зовнішні антропогенні фактори (Несанкціонований доступ до інформації, що захищається; несанкціоноване копіювання, зміна, видалення або блокування інформації, що захищається; дії кримінальних груп або окремих злочинних суб'єктів).

2. Внутрішні антропогенні фактори (Неправомірні дії осіб, які мають право доступу до інформації, що захищається; помилки в організаційному забезпеченні захисту інформації; помилки обслуговуючого персоналу; порушення конституційних прав і свобод людини і громадянина; вплив на парольно-ключові системи захисту автоматизованої системи обробки і передачі інформації; раптове відключення електрики).

3. Техногенні фактори (ПЕМВН; помилки і збої в роботі технічних засобів обробки інформації; помилки і збої в роботі програмного забезпечення).

4. Стихійні джерела (пожежі, урагани, блискавки).

1.3.2 Джерела загроз.

Джерела загроз поділяються на внутрішні і зовнішні.

До внутрішніх можна віднести:

- критичний стан організації;

- недостатня координація діяльності організації;

- неповний контроль керівництва за роботою співробітників;

- помилки персоналу, керівництва;

- збої, помилки програмно-технічних засобів і систем;

- продаж інформації.

До зовнішніх відносяться:

- діяльність конкурентів, фізичних або юридичних осіб, спрямована проти інтересів організації;

- загострення конкуренції за інформаційні технології та ресурси;

- діяльність терористичних організацій;

- Інтранет або Інтернет;

- несумлінні партнери, постачальники, клієнти, конкуренти;

- недостатня кількість кваліфікованих кадрів по забезпеченню інформаційної безпеки;

- форс-мажорні обставини (пожежа, землетрус, повінь (і т.д.);

- раптове відключення електрики, обрив проводу та ін.

1.3.3 Фізичне проникнення.

Дії зловмисника по добуванню інформації визначаються поставленими цілями і завданнями, його мотивами, кваліфікацією і технічною оснащеністю.

Модель зловмисника виглядає наступним чином:

- зловмисник представляє серйозного противника, ретельно готує операцію проникнення, вивчає: обстановку навколо території організації, які спостерігаються механічні перешкоди, засоби охорони, телевізійного спостереження і чергового (нічного) освітлення, а так само співробітників з метою добування від них інформації про способи і засоби захисту;

- має в розпорядженні сучасні технічні засоби проникнення і подолання механічних перешкод;

- усіма доступними способами добуває і аналізує інформацію розташуванні будівель і приміщень організації, про рубежах охорони, про місцях зберігання джерел інформації, видах і типах засобів охорони, телевізійного спостереження, освітлення і місцях їх установки;

- проводить аналіз можливих шляхів проникнення до джерел інформації та догляду після виконання завдання.

Залежно від кваліфікації, способів підготовки та фізичного проникнення в організацію зловмисників поділяють на такі типи:

- непідготовлений, який обмежується зовнішнім оглядом об'єкта, проникає в організацію через двері і вікна, при спрацювання тривожної сигналізації тікає;

- підготовлений, який вивчає систему охорони об'єкта і готує кілька варіантів проникнення в організацію, в основному шляхом злому інженерних конструкцій;

- кваліфікований, який ретельно готується до проникненням, виводить з ладу технічні засоби охорони, застосовує найбільш ефективні способи проникнення.

1.4. Збиток.

Імовірність проникнення зловмисника через вікно не велика, тому що по всьому периметру будівля оточена парканом, а також є система відео-спостереження.

Пролом стіни малоймовірний, тому що вимагає від зловмисника великий технічної підготовки і зробить багато шуму.

Проникнення через двері - найбільш простий шлях проникнення, з достатньою підготовкою пройти через КПП зловмисникові не складе особливих труднощів. Через двері можна проникнути будь-яким чином: отримавши ключі, або зламавши замок або двері або ж використовуючи якийсь інший шлях.

Землетрус малоймовірний, тому що в цьому районі дуже незначна сейсмічна активність.

Пожежа може завдати величезної шкоди, тому що може згоріти багато цінної інформації. Також варто врахувати збиток, нанесений водою, конкретно повені не буде, так як поблизу будівлі немає водойм, але існує можливість протікання труб і батарей.

Удар блискавки можливий, але малоймовірний.

1.5 Нормативно-правова база центру.

Керівництво і співробітники підприємства суворо дотримуються чинного законодавства. Відповідно до законів, комерційною таємницею є конфіденційність

інформації, що дозволяє її власникові при існуючих або можливих обставин збільшити доходи, уникнути невиправданих витрат, зберегти положення на ринку товарів, послуг або отримати іншу комерційну вигоду.

Існує наказ «Про порядок поводження з інформацією, що становить комерційну таємницю в ВАТ", в якому наведено перелік інформації, що становить комерційну таємницю ВАТ.

Перелік інформації, що становить комерційну таємницю ВАТ:

- інформація про фінансово-економічної діяльності;

- інформація про експлуатаційної та виробничої діяльності;

- інформація про управлінську діяльність;

- інформація про кадрову діяльності;

- інформація про контрольну і ревізійної діяльності;

- інформація про сигналізації і зв'язку, електрифікації, енергетиці;

- інформація про договірну роботу;

- інформація про результати власних досліджень;

- інформація про зовнішньоекономічну діяльність;

- інформація про рекламну діяльність;

- інформація про медичну діяльність;

- інформація про захист інформації і об'єктів ВАТ.

Режим комерційної таємниці визначений в законі як заходи, які вживає її володар для охорони її конфіденційності. Ці заходи носять правовий, організаційний, технічний і інший характер.

Доступом до інформації, що становить комерційну таємницю ВАТ і його контрагентів, є ознайомлення працівників ВАТ або третіх осіб з інформацією, що становить комерційну таємницю ВАТ і його контрагентів, за згодою ВАТ і його контрагентів або на законних підставах за умови збереження конфіденційності цієї інформації.

Відповідно до пункту закону «Про комерційну таємницю» працівник ВАТ, допущений до роботи з інформацією, що становить комерційну таємницю, зобов'язаний:

- виконувати вимоги цієї Інструкції та інших нормативних документів ВАТ встановлюють режим комерційної таємниці в ВАТ;

- не розголошувати інформацію, що становить комерційну таємницю, власниками якої є ВАТ і його контрагенти, і без їх згоди не використовувати цю інформацію в особистих цілях;

- не розголошувати інформацію, що становить комерційну таємницю, власниками якої є ВАТ і його контрагенти, після припинення трудового договору протягом трьох років;

- відшкодувати заподіяну ВАТ збиток, якщо працівник винен у розголошенні інформації, що становить комерційну таємницю, що стала йому відомою у зв'язку з виконанням ним трудових обов'язків;

- передати ВАТ при припиненні або розірванні трудового договору, наявні в користуванні працівника матеріальні носії інформації, що містять інформацію, що становить комерційну таємницю.

Відповідальність за встановлення в ВАТ режиму комерційної таємниці, виконання працівниками ВАТ вимог цієї Інструкції покладається на керівників ВАТ, керівників підрозділів ВАТ".

Відповідно до закону «Про комерційну таємницю» в трудових договорах з керівниками ВАТ, керівниками підрозділів ВАТ повинні передбачатися їх зобов'язання щодо забезпечення охорони конфіденційності інформації, власниками якої є ВАТ і його контрагенти, і відповідальність за забезпечення охорони її конфіденційності.

При розголошенні комерційної таємниці працівник зобов'язаний відшкодувати заподіяну роботодавцеві збиток, несе дисциплінарну, цивільно-правову, адміністративну та кримінальну відповідальність відповідно до законодавством за порушення встановлених в ВАТ вимог щодо захисту інформації, що становить комерційну таємницю ВАТ.

2. Розробка моделі КСЗІ підприємства.

**Мета 2:**

1. Описати входи КСЗІ - характеристика оброблюваних ресурсів і керуючих впливів.

2. Описати виходи КСЗІ - характеристика результатів функціонування.

3. Описати узагальнені властивості системи - продуктивність, стійкість, ефективність, адаптивність до змін у навколишньому середовищі (і т. д.). Характеристики можуть бути як кількісними, так і якісними.

4. Виділити системи навколишнього середовища (вищі організації, постачальники, споживачі, партнери, конкуренти (і т. д.). Дати їх коротку характеристику. Привести схему взаємодії досліджуваної КСЗІ з системами навколишнього середовища і описати взаємозв'язки.

Приклад виконання завдання

Першим найбільш простим і абстрактним рівнем описи системи є модель «чорного ящика». У цьому випадку передбачається, що виділена система пов'язана із середовищем через сукупність входів і виходів. Виходи моделі описують результати діяльності системи, а входи - ресурси і обмеження.

2.1 Входи і виходи системи захисту інформації.

Входи КСЗІ - це характеристика оброблюваних ресурсів і керуючих впливів.

На даному підприємстві входи КСЗІ будуть наступними:

- електроживлення;

- запити клієнтів (спільно із запитом клієнт повідомляє персональні дані);

- фінансова діяльність;

- ділова переписка;

- методи управління підприємством;

- персональні дані співробітників підприємства;

- безпеку підприємства;

Виходи КСЗІ - це характеристика результатів функціонування.

- технічні канали витоку інформації - мабуть, найважливіше, тому що за допомогою них передається інформація на інші підприємства, між співробітниками, начальству. Може статися знімання інформації від джерела до несанкціонованого одержувачу (наприклад, по акустичному каналу витоку, візуально-оптичному, радіоелектронного, електронного, матеріально-речового);

- фінансова звітність;

- укладання договорів з клієнтами та партнерами підприємства;

- політика безпеки;

- нормативна база підприємства по захисту інформації.

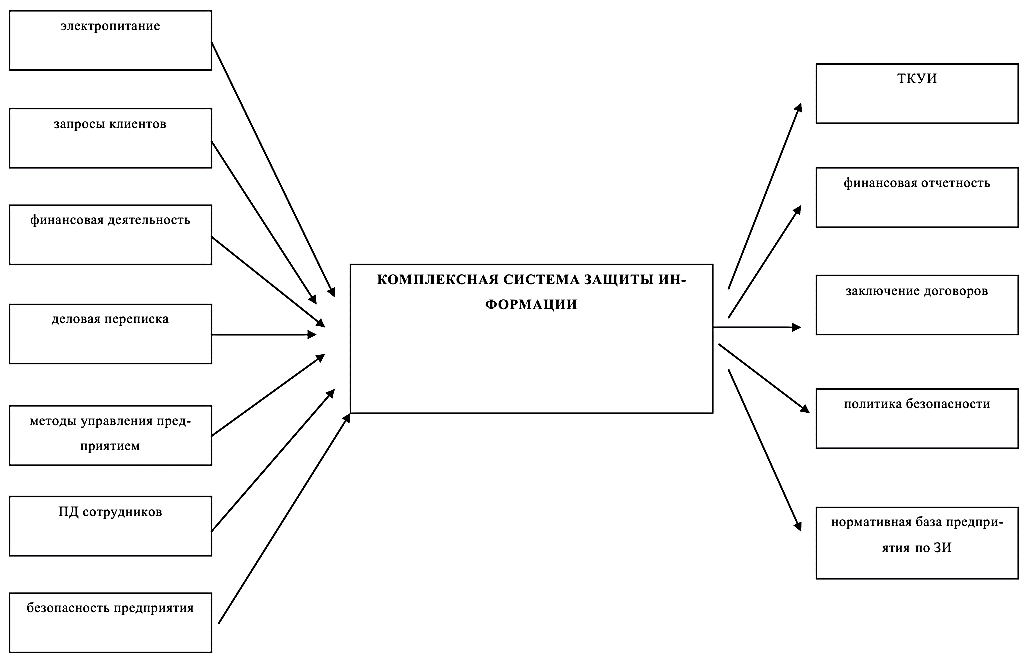


Рис. 2 Модель КСЗІ підприємства.

2.2 Узагальнені властивості системи.

Виділяють наступні узагальнені властивості системи захисту інформації:

- Ефективність. Ефективність забезпечується присутністю на підприємстві кваліфікованого фахівця із захисту інформації; дотримання

нормативних актів і законодавства в сфері захисту інформації.

- Продуктивність. Забезпечується застосуванням сучасних засобів обчислювальної техніки і створенням спеціально розробленого програмного забезпечення.

- Стійкість і відмовостійкість. Забезпечується за допомогою застосування систем резервного копіювання; веденням архівів копій документів.

- Адаптивність - можливість заміни окремих компонентів системи захисту, не порушуючи її структурної цілісності.

2.3 Системи навколишнього середовища.

До партнерів підприємства відносяться сам філія ВАТ, спеціальні видавництва, банки і т.д. Вони взаємодіють між собою на основі комерційних пропозицій.

Споживачі підприємства - юридичні та фізичні особи. Споживачі направляють запити підприємству, де вказують те, що їм необхідно зробити, беруть участь у формуванні попиту на ринку реклами, користуються послугами підприємства.

\*- Джерело інформації: Зырянова Т. Ю. Информационная безопасность: метод. указания / Т. Ю. Зырянова. – Екатеринбург: УрГУПС, 2015 – 33 с.