УДК 004.056: 378.4

ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХЕРСОНСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТА

Мазур А.В., Свєтланов І.Л.
Херсонський державний університет

У даній статті автори висвітлюють загальні проблеми інформаційної безпеки сучасної організації та аналізують актуальні питання комп'ютерної безпеки у Херсонському державному університеті.

***Ключові слова**: безпека, інформаційний, комп'ютер.*

Розвиток мережі Інтернет приводить до усвідомлення необхідності розширення організаціями своїх власних мереж та створенню гнучкої інфраструктури, адже це допомагає зацікавити більшу кількість клієнтів, значна частина яких при правильному підході потім може перетворитися із потенціальних на дійсних. Із цією метою організації, а освітні заклади тут не є виключенням, змушені відкривати доступ до власних інформаційних ресурсів, що неминуче призводить до зростання загрози прориву бар'єру інформаційно-технічного захисту із сторони зловмисників. Крім того, у будь-якому великому закладі, до числа яких можна віднести і Херсонський державний університет, існує розгалужена внутрішня система обміну та обробки даних у тому чи іншому вигляді, яка у наш час має вигляд єдиного комп'ютерного комплексу. Додаткова складність для підтримання необхідного рівня інформаційної безпеки обумовлюється у таких закладах, як правило, тим, що різні частини такої системі створюються у різний час із різними вимогами, а у якийсь момент робиться спроба їх об'єднати, що призводить до того, що не всі компоненти системи будуть відповідати вимогам безпеки. Звичайно, якщо організація створюється із самого початку із використанням правильного планування безпеки, націлюється на постійне проведення відповідних заходів, коли як керівництво, так і окремі члени організації усвідомлюють, чому це важливо, то, звичайно, у неї виникне мінімум відповідних проблем.

Але, як правило, організація створюється не заради того, щоб виконувати правила безпеки, а для того, щоб виконувати свої бізнес-завдання. Тому часто питання про безпеку постає лише тоді, коли вона у перший раз стикається із серйозними проблемами, такими, як втрата критично важливих даних, «епідемія» комп'ютерних вірусів, крадіжка важливої інформації зловмисниками тощо.

Отже, мета нашої статті – це, по-перше, зробити так, щоб читачі замислились над важливістю інформаційної безпеки до того, як виникне одна із вищезгаданих ситуацій, та, по-друге, оглянути ті елементи безпеки, які на даний момент існують у ХДУ, та роз'яснити особливості їх функціонування.

Спочатку зробимо короткий огляд «ідеальної» системи інформаційної безпеки.

Слід сказати, що усі нижченаведені правила та принципи були створені не в результаті абстрактних міркувань, а у результаті аналізу функціонування різноманітних організацій та тих викликів, із якими їм доводилося стикатись.

Отже, будь-яка організація повинна мати щонайменше наступні правила:

- Правила управління доступом:
  - управління реєстрацією та доступом
  - шифрування
  - інфраструктура відкритого ключа.
- Правила зовнішнього доступу
  - безпека Інтернет
  - доступ до віртуальної приватної мережі
  - Web та Internet

    - електронна пошта.
- Користувачі та правила фізичного захисту:
    - надійна робота
    - архітектура мережі та адресація
    - фізичний захист.

Тепер розглянемо детальніше ці пункти і подивимося, як вони реалізовані у Херсонському державному університеті.

Будь-які заходи по побудуванню системи інформаційної безпеки повинні починатися із визначення загальної політики безпеки, якої потім будуть дотримуватися усі члени виробничого процесу – як керівництво, так і окремі працівники організації. Підтримка керівництва грає значну роль, оскільки без неї ця політика не бути сприйматися серйозно і втілення її у життя буде приречене на невдачу із самого початку. І хоча підхід, при якому керівництво визначає, що кожен відтепер повинен нести відповідальність за безпеку на власній ділянці роботи, буде спрацьовувати якийсь час, це врешті-решт призведе до того, що розвиток установи буде стримуватися. Адже за умови використання різними відділами різних стандартів їх взаємодія буде проблематичною. А робота за єдиними стандартами безпеки призводить до того, що окремі структурні підрозділи організації починають працювати більш злагоджено. У ХДУ запроваджені «Правила експлуатації інформаційних систем університету», які є загальним документом, що визначає політику ХДУ у сфері інформаційної безпеки. У даному документі представлені загальні правила Херсонського державного університету, що регулюють роботу з інформаційними системами (надання доступу, збереження й обмін інформацією, контроль і розкриття різних електронних повідомлень, включаючи отримані і відправлені співробітниками Університету). Кожна з інформаційних систем може мати додаткові правила експлуатації, визначені в інших документах. Правила експлуатації інформаційних систем обов'язкові для всіх користувачів комп'ютерних і мережних систем Університету, включаючи співробітників, професорсько-викладацький і допоміжний персонал, а також інших осіб, що так або інакше експлуатують інформаційні системи Університету. Для співробітників Університету, яким наданий доступ до інформаційних систем, дані правила стають частиною їхніх функціональних обов'язків.

Керування засобами електронних комунікацій і інформаційних систем очолює проректор по інформаційним технологіям, міжнародним зв'язкам і соціально-економічним питанням. Крім того, між кількома відділами університету розподілено відповідальність за певні сфери безпеки. Центр комп'ютерних технологій відповідає за апаратне забезпечення серверної частини університету і програмне забезпечення всієї комп'ютерної техніки, прийнятої по акту введення в експлуатацію. Експлуатаційно-технічний відділ комп'ютерної техніки і зв'язку відповідає за апаратне і програмне забезпечення всіх навчальних комп'ютерних аудиторій та за апаратне забезпечення комп'ютерної техніки адміністративної мережі.

Фізична безпека – це перший ешелон інформаційного захисту будь-якої установи. По-перше, ключове обладнання повинне бути змонтоване у спеціальному приміщенні. У ХДУ таким приміщенням є серверна, яка обладнана системою кондиціювання повітря, яка підтримує постійну температуру усередині приміщення, яка необхідна для правильної роботи устаткування. У ідеалі двері мають бути вогнетривкими та герметичними, що призведе до мінімізації втрат у випадку виникнення пожежі, та не повинні бути постійно відкритими. По-друге, доступ до таких приміщень повинен мати доступ лише авторизований персонал (у нашому випадку – системний адміністратор). У великих установах із цією метою використовуються спеціальні засоби по управлінню доступом – перепустки, в тому числі електронні, реєстрація осіб, що працюють або відвідують установу. По-третє, повинні бути плани реагування на непередбачені обставини (не лише плани евакуації персоналу на випадок виникнення пожежі), на відновлення після аварії тощо. Установа повинна мати систему оповіщення про виниклу небезпеку. Крім того, повинен проводитися періодичний контроль стану та конфігурації інформаційної мережі.

Наступний крок – забезпечення безпеки мережі. Основний метод тут – використання автентифікації, коли особа отримує доступ до інформаційних ресурсів на підставі тих повноважень, які їх надані. Робота в локальній мережі ХДУ регулюється «Правилами експлуатації інформаційних систем університету». Так, вони, наприклад, визначають, що установка й настроювання мережних компонентів операційної системи, а також реєстрація комп'ютера в мережі Університету виконується тільки співробітниками центра комп'ютерних технологій; що користувачам заборонено змінювати настроювання мережних компонентів операційної системи; що головний адміністратор системи може відмовити в підключенні комп'ютера до інформаційної мережі університету, якщо програмні й технічні характеристики даного комп'ютера або пристрою не відповідають вимогам загальної безпеки інформаційної мережі університету; що користувачі не повинні перешкоджати роботі сценаріїв, виконуваних на їхніх комп'ютерах при реєстрації у мережі Університету. Користувачу або відділу може бути надана папка на сервері для збереження особистої і службової інформації. Інформація Університету є його власністю і не повинна передаватися стороннім особам. У разі потреби для виконання своїх виробничих задач користувач може копіювати цю інформацію, передавати цю інформацію можна тільки відповідному персоналу.

Для управління доступу до мережі ХДУ використовуються технології доступу Microsoft, вбудовані у відповідні продукти. Права доступу визначаються при реєстрації користувачів відповідно до існуючих правил. У ХДУ також проводиться роз’яснення того, до яких саме інформаційних ресурсів і на яких умовах надається доступ. Це необхідно не лише для організації доступу до них користувачів, але й для захисту персональної інформації про працівників, яка захищена законодавством України. Отож, потрібні правила та система, що установлює порядок доступу до такої інформації. У ХДУ такі ресурси містить Інформаційно-аналітична система (ІАС) – програма, що дозволяє вести облік працівників (адреса, кваліфікація, посада, відпустки, заробітна платня, шпитальні листи, реєстрація, пільги, тривалість виконання робочих завдань) і студентів (вступ, спеціальність, випуск, розподіл, академічні відпустки, накази), бухгалтерський облік, контроль за матеріальними цінностями. Доступ до неї регулюється відповідними правилами.

У організаціях, де працівникам дозволяється виконувати свої обов’язки, не знаходячись при цьому безпосередньо на робочих місцях, також повинні існувати правила доступу до локальної мережі за допомогою VPN.

Internet у наш час – потужній робочий засіб, який у той же час може бути джерелом багатьох проблем, пов’язаних із інформаційною безпекою, тому відповідні правила слід розробляти особливо ретельно. У ХДУ ці питання регулюють «Правила експлуатації інформаційних систем університету». У них визначено, що університет створює й підтримує інфраструктуру, що забезпечує доступ користувачів в Internet, перелічені апаратні та програмні вимоги до комп’ютерів, яким може бути наданий такий доступ, та містяться деякі специфічні вимоги. Так, наприклад, користувачам заборонено змінювати настроювання підключення, безпеки і використовуваних програм браузера без дозволу керівництва Університету. Підключення Університету до Internet повинно використовуватися лише для виробничих цілей. Час доступу співробітників в Internet визначається регламентом роботи Університету. Користувачі не повинні передавати по Internet ніяку інформацію, розголошення якої може нанести шкоду їм особисто або Університету. Користувачі, яким надане право завантажувати програмне забезпечення з Internet, повинні робити це на системах, захищених постійно обновлюваним антивірусним програмним забезпеченням. Антивірусне програмне забезпечення повинне знаходитись в робочому стані, коли завантажене ззовні програмне забезпечення запускається на комп'ютері користувача.

Крім вищенаведених, повинні також існувати правила електронної торгівлі (сюди відносяться правила зберігання даних, захист пересилання даних та методи обробки заказів), якщо організація використовує її у своїх бізнес-процесах. На даний момент ХДУ не використовує такі можливості.

Одним із найбільш поширених засобів спілкування залишається електронна пошта, яка дозволяє пересилати повідомлення майже блискавично. ХДУ має власноруч розроблені правила, що регламентують роботу із електронною поштою та службами миттєвих повідомлень. У них визначено, що університет створює, керує й підтримує інфраструктуру, що забезпечує доставку електронної пошти й інших повідомлень користувачам усередині Університету й іншим особам через Internet. Для користувачів, яким надане право використання електронної пошти, на сервері створюється поштова скринька. Користувачі повинні чітко розуміти, що надана їм у користування електронна адреса є власністю Університету і її функціонування може бути припинене в будь-який момент без погодження з користувачем. Для доступу до ресурсів електронної пошти повинна використовуватися програма MS Outlook, настроєна на корпоративний режим роботи з поштою. Користувачам заборонено самостійно змінювати настроювання програми без дозволу керівництва Університету. Користувачі повинні регулярно перевіряти і негайно відповідати на адресовану їм службову електронну кореспонденцію. Секретна чи конфіденційна інформація може відправлятися тільки користувачам, що має доступ до локальної мережі. Користувачі не повинні підписуватися на списки розсилання, що не мають безпосереднього відношення до діяльності Університету, оскільки одержання й переадресація таких повідомлень приводить до значного завантаження внутрішнього поштового сервера. Користувачі електронної пошти й служб миттєвих повідомлень повинні дотримувати загальні правила етикету.

Слід сказати, що ХДУ має власний WEB-сайт, який надає доступ до актуальної інформації, що стосується усіх його підрозділів, кожен із яких може редагувати свою сторінку. Робота із даним ресурсом регламентується «Положенням про Web-портал Херсонського державного університету», у яких, зокрема, йдеться про те, що сайт ХДУ забезпечує офіційне подання інформації про університет у мережі Інтернет. Користувачем сайту може бути будь-яка особа, яка має технічні можливості виходу в Інтернет. Інформаційне наповнення та актуалізація сайту здійснюється спільними зусиллями ректорату, інститутів, факультетів, кафедр, структурних підрозділів, а також громадських організацій університету. По кожному розділу сайту (виду інформаційного ресурсу) визначаються підрозділи (посадові особи), відповідальні за добірку й надання відповідної інформації. За зміст опублікованих матеріалів відповідальність несе та структурна одиниця, яка їх публікує. Доступ для самостійного розміщення матеріалів підрозділами надається адміністратором після узгодження з проректором з науково-педагогічної роботи, інформаційних технологій, міжнародних зв’язків (подання заявки).

Наступний крок – антивірусна безпека. На жаль, у наш час нові віруси, «трояни» та шкідливі програми з’являються майже кожен тиждень. Вони можуть призвести як до незначних проблем, так і до призупинення роботи усієї мережі, що є неприпустимим. В ХДУ антивірусна безпека визначається «Правилами експлуатації інформаційних систем університету» та наказом «Про посилення внутрішньої антивірусної безпеки у мережі університету». Ці правила визначають, що користувачі відповідають за відсутність вірусів на закріплених за ними комп'ютерах. Якщо користувачу Університетом надані антивірусні засоби, він зобов'язаний проводити антивірусну перевірку усієї вхідної і вихідної інформації. Користувачам заборонено навмисно створювати, виконувати, поширювати або встановлювати комп'ютерні програми, які можуть самовідтворюватися, викликати ушкодження чи ускладнювати роботу оперативної пам'яті, пристроїв, що запам'ятовують, операційних систем або іншого програмного забезпечення. Користувачі не повинні запускати або відкривати будь-як файли (у тому числі файли документів MS Word, MS Excel), прикріплені до повідомлень електронної пошти, попередньо не перевіривши їх за допомогою антивірусного програмного забезпечення. Програмне забезпечення й інші файли не можна завантажувати або встановлювати на комп'ютери Університету, поки вони не будуть перевірені антивірусним програмним забезпеченням.

У останній час ХДУ купує комерційні антивірусні продукти, такі як KAV, які забезпечують безпеку серверів та певної кількості робочих станцій.

Одним із ефективних методів забезпечення цілісності та недоторканості даних, що пересилаються через Internet або використовуються для роботи, є шифрування. У ХДУ користувачі мають право використовувати шифрувальне програмне забезпечення, надане їм адміністратором системи чи розроблювачами відповідного програмного забезпечення з метою захисту ділової конфіденційної інформації. Користувачі, що використовують шифрування файлів або архівів, що зберігаються на кожному з комп'ютерів Університету, зобов'язані повідомити про це системного адміністратора і повинні забезпечити його паперовою роздруківкою всіх паролів або ключів шифрування, необхідних для доступу до файлу/архіву. Користувачам, що використовують шифрування, варто прийняти також усі інші, описані в документації програмного забезпечення міри, необхідні для можливості аварійного відновлення зашифрованого файлу/архіву. Усі дискети, використовувані для функціонування шифрувальних програм, повинні зберігатися в сейфі і вийматися звідти лише тоді, коли це необхідно.

Оскільки деякі відділи ХДУ, зокрема, Науково-дослідний інститут інформаційних технологій, займаються розробкою програмного забезпечення, то є потреба мати певні правила, які б регулювали цей вид діяльності. Одним із кроків на цьому шляху стала підготовка сертифікації Інституту на відповідність стандартам ISO-9001. На даний момент робота інституту ведеться згідно з системою якості, яка забезпечує високу якість продукту. Це досягається шляхом документування процесів та їх взаємодій; навчанням персоналу та надаванням ресурсів, що необхідні для нормального виконання процесу; постійного слідкування за процесами та виконання коригувальних дій для отримання запланованих результатів; постійного пошуку шляхів вдосконалення процесу розробки та впровадження покращань.

Отже, у ХДУ існують певні компоненти системи інформаційної безпеки, але на даний момент вони не можуть забезпечити максимальний рівень захисту університету від сучасних викликів. Так, хоча в університеті впроваджена, наприклад, реєстрація користувачів та розмежовування доступу до інформаційних ресурсів, існують правила використанні Internet та електронної пошти, разом із тим не проводяться регулярні перевірки конфігурації та стану мережі, немає надійного механізму архівації та резервування даних, відсутній спеціальний відділ, який би займався координацією та контролем за додержанням правил безпеки.

На жаль, обсяг даної статті не дозволяє провести ретельний аналіз усіх питань інформаційної безпеки та їх реалізації у Херсонському державному університеті. Втім, ми намагалися зробити лише стислий огляд та підкреслити ті моменти, на які слід звернути увагу, щоб зробити систему інформаційної безпеки в ХДУ більш ефективною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Белов Е.Б., Лось В.П. Основы информационной безопасности.
2. Вильям Столлингс. Основы защиты сетей. Приложения и стандарты. Изд. «Вильямс», 2002.
3. Герасименко В.А. «Защита информации в автоматизированных системах обработки данных» Москва, Энергоатомиздат 1994 г.
4. Скотт Бармен. Разработка правил информационной безопасности. М., 2002.
5. Стивен Норткат, Джуди Новак. Обнаружение нарушений безопасности в сетях. Изд. «Вильямс», 2003.