ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Анализ угроз объекту информационной безопасности

Федоров Дмитрий Николаевич
dnf@dnf.su

III

РАЗДЕЛЫ ТЕМЫ

- Понятие угрозы и ее основные свойства
- Классификация угроз. Ущерб информационной безопасности предприятия.

Раздел 1

ПОНЯТИЕ УГРОЗЫ И ЕЕ ОСНОВНЫЕ СВОЙСТВА

ВВЕДЕНИЕ

- Понятие «обеспечение **информационной безопасности**» включает объекты информационной безопасности, угрозы объектам информационной безопасности и деятельность по защите этих объектов, основанную на совокупности сил, средств, способов и методов обеспечения **информационной безопасности**.
- Главными целями деятельности по обеспечению **информационной безопасности**, как уже отмечалось, являются ликвидация угроз объектам информационной безопасности и минимизация возможного ущерба, который может быть нанесен вследствие реализации данных угроз.
- Рассмотрим сущность и основные виды **угроз информационной безопасности**.

ПОНЯТИЕ УГРОЗЫ

- Угроза — одно из ключевых понятий в сфере обеспечения информационной безопасности.
- **Угроза объекту информационной безопасности** есть совокупность факторов и условий, возникающих в процессе взаимодействия различных объектов (их элементов) и способных оказывать негативное воздействие на конкретный объект **информационной безопасности**.
- Негативные воздействия различаются по характеру наносимого вреда, а именно:
  - по степени изменения свойств объекта безопасности
  - по возможности ликвидации последствий проявления угрозы.

СВОЙСТВА УГРОЗЫ

- Избирательность характеризует нацеленность угрозы на нанесение вреда тем или иным конкретным свойствам **объекта безопасности**.
- Предсказуемость характеризует наличие признаков возникновения угрозы, позволяющих заранее прогнозировать возможность появления угрозы и определять конкретные **объекты безопасности**, на которые она будет направлена.
- Вредоносность характеризует возможность нанесения вреда различной тяжести объекту безопасности. Вред, как правило, может быть оценен стоимостью затрат на ликвидацию последствий проявления угрозы либо на предотвращение ее появления.

ТИПЫ УГРОЗ И ИХ ОСОБЕННОСТИ

- Намерение нанести вред, которое появляется в виде объявленного мотива деятельности субъекта.
  - Особенность первого типа угроз заключается в неопределенности возможных последствий, неясности вопроса о наличии у угрожающего субъекта сил и средств, достаточных для осуществления намерения.
- Возможность нанесения вреда – существование достаточных для этого условий и факторов.
  - Возможность нанесения вреда заключается в существовании достаточных для этого условий и факторов. Особенность угроз данного типа состоит в том, что оценка потенциала совокупности факторов, которые могут послужить превращению этих возможностей и условий во вред, может быть осуществлена только собственно субъектами угроз.

ПРИЧИННО-СЛЕДСТВЕННАЯ СВЯЗЬ «УГРОЗЫ» И «ОПАСНОСТИ»

- Угроза всегда порождает опасность.
- Опасность также можно представить как состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту.
- Главное отличие между ними заключается в том, что опасность является свойством объекта информационной безопасности и характеризует его способность противостоять проявлению угроз, а угроза – свойством объекта взаимодействия или находящихся во взаимодействии элементов объекта безопасности, выступающих в качестве источника угроз.
- Понятие угрозы имеет причинно-следственную связь не только с понятием опасности, но и с возможным вредом как последствием негативного изменения условий существования объекта. Возможный вред определяет величину опасности.

Раздел 2

КЛАССИФИКАЦИЯ УГРОЗ. УЩЕРБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.

ВИДЫ КЛАССИФИКАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА (1 ИЗ 3)

1. по источнику (его местонахождению) – на:
   - внутренние (возникают непосредственно на объекте и обусловлены взаимодействием между его элементами или субъектами) и
   - внешние (возникают вследствие его взаимодействия с внешними объектами);
2. по вероятности реализации – на потенциальные и реальные;
3. по размерам наносимого ущерба – на:
   - общие (наносят вред объекту безопасности в целом, оказывая существенное негативное воздействия на условия его деятельности),
   - локальные (затрагивают условия существования отдельных элементов объекта безопасности) и
   - частные (наносят вред отдельным свойствам элементов объекта или отдельным направлениям его деятельности);

ВИДЫ КЛАССИФИКАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА (2 ИЗ 3)

4. по природе происхождения – на:
   - случайные (не связанные с действиями персонала, состоянием и функционированием объекта **информационной безопасности**, такие как отказы, сбои и ошибки в работе средств автоматизации, стихийные бедствия и другие чрезвычайные обстоятельства) и
   - преднамеренные (обусловлены злоумышленными действиями людей);
5. по предпосылкам возникновения – на:
   - объективные (вызваны недостатком **системы информационной безопасности** объекта, например, несовершенством разработанных нормативно-методических и организационно-плановых документов, отсутствием подготовленных специалистов по **защите информации** и т.п.) и
   - субъективные (обусловлены деятельностью персонала объекта безопасности, например, ошибками в работе, низким уровнем подготовки в **вопросах защиты информации**, злоумышленными действиями или намерениями посторонних лиц);

ВИДЫ КЛАССИФИКАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА (3 ИЗ 3)

6. по видам объектов безопасности – на:
   - угрозы собственно информации (обусловлены попытками получения защищаемой информации различными способами и методами независимо от ее местонахождения),
   - угрозы персоналу объекта (связаны с уменьшением влияния персонала на ситуацию в сфере обеспечения информационной безопасности, с попытками получения конфиденциальной информации от допущенного к ней персонала),
   - угрозы деятельности по обеспечению информационной безопасности (направлены на снижение эффективности или нейтрализацию усилий, предпринимаемых руководством и персоналом объекта безопасности для исключения утечки защищаемых сведений, утраты или хищения носителей, ослабление системы защиты информации).

КЛАССИФИКАЦИЯ ПОДЛЕЖАЩИХ ЗАЩИТЕ ОБЪЕКТОВ

- При рассмотрении угроз информационной безопасности объекта особое внимание необходимо уделить классификации подлежащих защите объектов **информационной безопасности** предприятия.
- В соответствии с приведенной ранее классификацией угроз по виду объекта воздействия они подразделяются на:
  - угрозы собственно информации,
  - угрозы персоналу объекта и
  - угрозы деятельности по обеспечению информационной безопасности объекта.
- При более детальном рассмотрении угрозы собственно информации можно подразделить на:
  - угрозы носителям конфиденциальной информации,
  - местам их размещения (расположения),
  - каналам передачи (системам информационного обмена), а также
  - собственно информации, хранящейся в документированном (электронном) виде на различных носителях.

УЩЕРБ КАК ДЕЙСТВИЕ УГРОЗ

- Вывод 1: Действие **угроз информационной безопасности** объекта направлено на:
  - создание возможных каналов **утечки защищаемой информации** (предпосылок к ее утечке) и
  - непосредственно на **утечку информации**.
- Одно из ключевых понятий в оценке эффективности проявления угроз объекту информационной безопасности — ущерб, наносимый этому объекту (предприятию) в результате воздействия угроз.
- По своей сути любой ущерб, его определение и оценка имеют ярко выраженную экономическую основу. Не является исключением и ущерб, наносимый информационной безопасности объекта (предприятия).

ЭКОНОМИЧЕСКАЯ ОЦЕНКА УЩЕРБА

- С позиции экономического подхода общий **ущерб информационной безопасности** предприятия складывается из двух составных частей:
  - Прямого, который возникает вследствие утечки конфиденциальной информации.
  - Косвенного ущерба - потерь, которые несет предприятие в связи с ограничениями на распространение информации, в установленном порядке отнесенной к категории конфиденциальной.
- Описание ущерба, наносимого предприятию в результате утечки конфиденциальной информации, основывается на его количественных и качественных показателях, которые базируются на одном из принципов засекречивания информации (отнесения ее к категории конфиденциальной) — принципе обоснованности.
- Он заключается в установлении (путем экспертных оценок) целесообразности засекречивания конкретных сведений (отнесения содержащейся в них информации к категории конфиденциальной), а также вероятных последствий этих действий, с учетом решаемых предприятием задач и поставленных целей.

«+» И «–» ОГРАНИЧЕНИЙ НА РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ

- Введение ограничений на распространение информации (в связи с ее засекречиванием или отнесением к категории конфиденциальной) приводит и к позитивным, и к негативным последствиям.
- К основным позитивным последствиям следует отнести предотвращение возможного прямого ущерба информационной безопасности предприятия из-за утечки защищаемой информации.
- Негативные последствия связаны с наличием (вероятным возрастанием) косвенного ущерба или издержек в виде затрат на **защиту информации** и величины упущенной выгоды, которая может быть получена при ее открытом распространении.

ОЦЕНКА ОБЩЕГО УЩЕРБА

- Общий ущерб безопасности предприятия от утечки конфиденциальной информации определяют следующим образом:
- Проводят классификацию всех имеющихся на предприятии сведений по степени их важности. С этой целью методом экспертной оценки с привлечением специалистов структурных подразделений предприятия, участвующих в выполнении работ по различным направлениям его деятельности, разрабатывают единую шкалу сведений, содержащих конфиденциальную информацию — так называемый рейтинг важности информации. В рейтинге отражаются все сведения, включенные в перечни информации, подлежащей защите.
- Методической основой для разработки такого рейтинга служит метод экспертного анализа в совокупности с методом объективного количественного оценивания. На основе рейтинга важности информации сопоставляют (соотносят) включенные в него сведения с количественными показателями возможного ущерба, определяемого расчетным или экспертным путем.

Все материалы курса доступны для зарегистрированных пользователей Академии современных инфокоммуникационных технологий «АСИКТ»
www.acikt.ru