Лекция 3. Организация защиты информации. Организационные меры ЗИ

Цель лекции: Ознакомить студентов с мерами обеспечения защиты информации. Рассмотреть организационные меры защиты информации

План лекции:

1. Организация защиты информации.
2. Организационные меры ЗИ

Первым объектом нашего сегодняшнего разговора станет организация защиты информации. Мы обсудим некие принципиальные моменты построения системы защиты информации в организации. Для чего же, собственно, строится система защиты информации, каких целей стремятся достичь специалисты по защите информации, предпринимая различные меры и усилия? Прежде всего, стремятся снизить вероятность техногенных угроз. Практически любая автоматизированная система, располагающаяся на территории объекта информатизации, подвержена техногенным угрозам, то есть различным сбоям, выходам из строя оборудования, которые неизбежно приводят к нарушению, например, доступности информации в случае, если носитель информации полностью уничтожается. Либо сбои могут приводить к нарушению целостности, если в информацию вносятся случайные искажения по причине каких-то аппаратных ошибок и программных сбоев или наоборот — аппаратных сбоев и программных ошибок. После того как вероятность техногенных угроз снижена, следующей целью, которую желательно достичь, является снижение ущерба от стихийных явлений. Опять же, практически любой объект информатизации им подвержен, даже самая небольшая организация не застрахована от наводнений, пожаров, различных подобного рода явлений, которые могут повлиять на здание, в котором она располагается. Поэтому снижение ущерба от стихийных явлений — ещё одна цель, которую желательно достичь. Далее, следующая цель по нарастанию — снижение вероятности угроз, реализуемых по причине халатности или недостаточной квалификации. Наконец, доходит очередь до нарушителей, действующих из любопытства или самоутверждения, опять же практически в любой организации нельзя исключать их наличия. Ну и наконец, после того как какие-то минимальные меры защиты, защищающие от таких, скажем так, нецеленаправленных нарушителей, реализованы, последним этапом является защита от нарушителей, действующих преднамеренно и целенаправленно, то есть уже от серьёзных угроз и от серьёзных нарушителей, которые появляются действительно при построении модели каких-то крупных или важных объектов информатизации, представляющих собой государственные учреждения, крупные коммерческие структуры, различные прибыльные организации,

которые могут привлечь внимание конкурентов и подобных объектов информатизации.

Среди различных категорий мер защиты информации мы выделим с вами следующие.

Во-первых, **организационные меры защиты** информации в широком смысле — это такие меры обеспечения защиты информации, которые представляют собой любые действующие на территории объекта информатизации правила, которые управляют доступом к информации, порядком работы с ней, а также в совокупности с этими правилами и меры обеспечения контроля исполнения таких правил. То есть и пропускной режим, и разграничения доступа пользователей в различные помещения и конформации, и регламент того, как должен предоставляться доступ к информации посетителям или клиентам организации, всё это попадает в эту категорию.

Организация защиты информации — совокупность действий, направленных на выявление угроз безопасности информации, планирование, реализацию мероприятий по защите информации и контроль состояния защиты информации.

Организационные меры защиты информации в ряде источников разделяются на законодательные меры защиты информации, административные меры защиты информации, организационно-технические меры защиты информации, и иногда ещё выделяются морально-этические меры защиты информации.

Следующий класс, который мы рассмотрим, это **криптографические меры** защиты информации, также в широком смысле. Под ними будем понимать меры обеспечения защиты информации, представляющие собой преобразование информации, как правило, на основе секретного параметра, так, чтобы использовать эту информацию и получать к ней доступ могло только лицо, которое этим секретом владеет. Криптографические меры защиты информации включают алгоритмы шифрования, функции хэширования и схемы электронной цифровой подписи. Криптографические меры защиты информации, как, впрочем и часть организационных мер защиты информации, будут предметом отдельной лекции в дальнейшем в пределах нашего курса.

Следующий класс — это **меры технической защиты информации**. Это меры обеспечения защиты информации от несанкционированного доступа с использованием приёмов технической разведки. Заключаются они в защите информации от утечек по техническим каналам утечки информации, и такие каналы основываются на физических основах процессов обработки и передачи информации пользователями и техническими средствами. Такие меры включают, как правило, специальное оснащение объекта информатизации, применение специфических средств защиты от несанкционированного съёма информации. Обычно для повышения их эффективности они применяются в комплексе с организационными мерами защиты информации, не ограничиваясь

просто инструктированием пользователей по использованию таких средств защиты технической информации, но и включая также регламент использования пользователями различных объектов информации, проведения переговоров и подобного рода мероприятий.

Четвёртый крупный класс, который мы рассмотрим, это **стеганографические меры защиты информации**. Это меры обеспечения защиты информации, направленные на сохранение в секрете самого обстоятельства передачи информации или факт её наличия от всех лиц, не являющихся легальными пользователями информации.

В ряде источников также выделяется такой обобщённый класс, как **программно-технические меры защиты информации**. Под ними подразумеваются меры обеспечения защиты информации, заключающиеся в использовании специальных программных, аппаратных и программно-аппаратных средств, входящих в состав информационной системы. Некий изъян такой классификации, в смысле выделения этого класса, заключается в том, что в него попадают любые по принципу действия средства информационной безопасности без раскрытия того, что же положено в их принцип: это и программная реализация шифрования, и программная реализация стеганографических мер защиты информации и любые иные программные и программно-аппаратные комплексы, они в этот класс попадают. Тем не менее понятие программно-технических мер защиты встречается во многих источниках, и мы его тоже рассматриваем.

Таким образом, мы получаем две классификации. По принципу действия выделяем четыре больших класса — это организационные меры защиты информации, это любые правила и регламенты, криптографические меры защиты информации (преобразования на основе преобразований ключа), меры технической защиты информации (защиту от утечек по физическим каналам) и стеганографические меры зашиты информации (меры сокрытия самой информации или её передачи). Зачем требуется скрывать факт наличия информации или её передачи, мы уже в сегодняшней лекции этот вопрос затронем. И вторая классификация — это по способам осуществления, то есть по тому, что собой представляют меры защиты информации. Законодательные — то есть оформленные в виде каких-то актов правительства, морально-этические меры защиты информации — не являющиеся обязательными сложившиеся своды правил, кодексы поведения, нормативы, просто неписаные нормы, действующие в обществе.

Например, в тех или иных учреждениях, в которых клиенты могут озвучивать свои персональные данные, например в банках, хорошим тоном является предлагать клиенту написать на листочке фамилию, имя, отчество для открытия вклада и для написания суммы для внесения на счет. Не очень хорошим, когда посетителя просят проговорить эти данные вслух, например, назвать свой номер телефона. Вот пример морально-этической меры зашиты

информации. Административные меры защиты информации — это различные регламенты и решения, и правила, установленные руководством организации. Организационно-технические меры защиты информации — это меры защиты информации, предполагающие собственно обеспечение принятых на территории объекта информатизации правил, то есть физическая защита объекта информатизации, контроль доступа на его территорию и сотрудников в различные помещения. И наконец, программно-технические меры защиты — это любые по принципу действия программные, технические или программно-технически и программно-аппаратные комплексы.

Если сопоставлять эти две классификации, получится примерно такая таблица сопоставления: организационные меры защиты информации в широком смысле включают в себя четыре категории из классификации по способам осуществления, зато наоборот, в класс программно-технических мер защиты информации можно поместить программные или программно-аппаратные реализации криптографических мер защиты информации, мер технической защиты информации и стеганографические меры защиты информации.

Рассмотрим подробнее организационные меры защиты информации. **Организационные меры защиты информации** по своей сути выполняют следующие задачи. Они регламентируют действия персонала автоматизированной системы объекта информатизации, регламентируют порядок доступа иных субъектов к информации, обрабатываемой на объекте информатизации, то есть посетителей, клиентов, лиц, привлекаемых для пусконаладочных устройств различного оборудования, сотрудников организаций, предоставляющих, например, услуги подключения к сети Интернет, то есть провайдера, услуги телефонной связи, прочих видов связи, а также различных служб, осуществляющих обслуживание поддерживающей инфраструктуры, то есть системы отопления, системы электроснабжения, и прочих лиц. А также организационные меры создают условия обеспечения и контроля соблюдения регламентов и правил. Они предназначены для обеспечения всех трех свойств защищаемой информации: целостности, доступности и конфиденциальности, но, как правило, на достаточно слабом уровне, достаточном для того, чтобы противостоять угрозам нарушителя, не ставящего своей целью непременно реализовать угрозу по отношению к конкретному объекту информатизации, то есть для того, чтобы отсечь угрозы, реализуемые по халатности или недостаточной квалификации, а также нарушителей, действующих из самоутверждения и интереса, не слишком заинтересованных в достижении своей целей.

Существуют ситуации, когда нарушитель, действующий из интереса и для самоутверждения, напротив, проявляет большое упорство в достижении своей

цели и может оказаться действительно серьезной угрозой. Но, в большинстве случаев, если нарушители просто пытаются в массе объектов информатизации найти какие-то уязвимые места, то таких организационных мер, как правило, достаточно для того, чтобы большинство из них потеряло интерес к конкретному объекту информатизации и перестало бы предпринимать попытки реализовывать угрозу. Организационные меры защиты информации, как правило, эффективны для снижения вероятности техногенных угроз за счет регламентирования действий пользователя, за счет обучения пользователей информационной системы, как следует правильно себя вести в случае возникновения подобных угроз, за счет предусмотрения копирования, может быть, дублирования ключевых узлов информационной системы, и подобных решений; для снижения ущерба от стихийных явлений, аналогичным образом путем разработки порядка действий персонала на случай этих стихийных явлений, путем создания резервных копий, возможно в удаленном хранилище, арендованном у другой организации, что позволяет избежать, например, нарушения доступности информации. То есть если на территории объекта информатизации возможно осуществление какого-то стихийного явления, например пожара, то, возможно, разумным будет регулярно обеспечивать резервное копирование на носителях информации, арендованных в другой организации, например в облачном хранилище. В этом случае, если носители информации будут физически уничтожены (те, которые располагаются на территории объекта информатизации), то возможно будет восстановить информацию из резервной копии, и, например, база данных не будет полностью утрачена.

Также такие меры могут оказаться недостаточными для противодействия внутреннему нарушителю, действующему злоумышленно, то есть уже имеющему легальный доступ на территорию объекта информатизации и при этом способного вступать в сговор с другими пользователями информационной системы, способного действовать достаточно открыто и в рамках своих полномочий. При этом если он действует злоумышленно, то есть не просто по халатности, и сознательно нарушает регламенты и правила своих действий, то, разумеется, организационные меры могут оказаться от него бессильны, хотя некоторые их сочетания могут ему успешно противостоять. А также такие меры недостаточны для проведения техногенным угрозам нарушения целостности информации на контролируемой территории объекта информатизации. Также организационные меры защиты информации в отдельных случаях могут оказаться недостаточными для противодействия техногенным угрозам нарушения целостности информации на контролируемой территории объекта информатизации. Здесь речь идет о незамеченных программных сбоях,

приводящих к искажению информации, например в базах данных, в случае экстренного отключения подачи электроэнергии. Если в результате этого случилась какая-то ошибка и в базе данных случилось искажение, которое не было замечено самими пользователями, то организационных мер защиты информации может оказаться недостаточно.

Организационная защита объектов информатизации

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц;
- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учёт, исполнение, возврат, хранение и уничтожение;
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению её защиты;
- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учёта, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.

2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.

3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.

4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582

5. Организационная безопасность на предприятии: бумажная и практическая безопасность. inforsec.ru. Дата обращения: 13 сентября 2021.