Тема :
«Понятие информационной безопасности в РФ»

Для специальностей: 09.02.01,09.02.02,09.02.03,09.02.04

Преподаватель ГБПОУ МАДК им. А. А. Николаева

Батенина М. Ю.

Содержание :

- Понятие информационной безопасности
- Механизмы информационной безопасности
- Инструментарий информационной безопасности
- Основные направления информационной безопасности
- Терминология
- Задачи службы информационной безопасности
- Чем должна заниматься служба безопасности
- Сфера охвата информационных систем
- Сфера охвата персонала
- Сфера охвата проектов
- Контроль функционирования службы
- Создание службы безопасности
- Состав службы информационной безопасности
- Уровень подготовки специалистов
- Законодательство

Понятия

- **Информационная безопасность** — это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:
  Конфиденциальность — возможность ознакомиться с информацией (именно с данными или сведениями, несущими смысловую нагрузку, а не с последовательностью бит их представляющих) имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями;
  Целостность — возможность внести изменение в информацию (опять речь идет о смысловом выражении) должны иметь только те лица, кто на это уполномочен;
  Доступность — возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.

Механизмы

- **Политика** — набор формальных (официально утвержденных либо традиционно сложившихся) правил, которые регламентируют функционирование механизма информационной безопасности;
  Идентификация — определение (распознавание) каждого участника процесса информационного взаимодействия перед тем как к нему будут применены какие бы то ни было понятия информационной безопасности;
  Аутентификация — обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно, т. е. действительно является тем, чей идентификатор он предъявил;
  Контроль доступа — создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа;

- **Авторизация** — формирование профиля прав для конкретного участника процесса информационного обмена (аутентифицированного или анонимного) из набора правил контроля доступа;

  Аудит и мониторинг — регулярное отслеживание событий, происходящих в процессе обмена информацией, с регистрацией и анализом предопределенных значимых или подозрительных событий. Понятия "аудит" и "мониторинг" при этом несколько различаются, так как первое предполагает анализ событий постфактум, а второе приближено к режиму реального времени;

Реагирование на инциденты — совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности;

Управление конфигурацией — создание и поддержание функционирования среды информационного обмена в работоспособном состоянии и в соответствии с требованиями информационной безопасности;

Управление пользователями — обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями информационной безопасности.

Инструментарий

- *Перечислим основные средства (инструменты) информационной безопасности:*

Персонал — люди, которые будут обеспечивать претворение в жизнь информационной безопасности во всех аспектах, то есть разрабатывать, внедрять, поддерживать, контролировать и исполнять;

Нормативное обеспечение — документы, которые создают правовое пространство для функционирования информационной безопасности;

Модели безопасности — схемы обеспечения информационной безопасности, заложенные в данную конкретную информационную систему или среду;

Криптография — методы и средства преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию), вместе с методами и средствами создания, хранения и распространения ключей — специальных информационных объектов, реализующих эти санкции;

- **Антивирусное обеспечение** — средство для обнаружения и уничтожения зловредного кода (вирусов, троянских программ и т. п.);
- **Межсетевые экраны** — устройства контроля доступа из одной информационной сети в другую;
- **Сканеры безопасности** — устройства проверки качества функционирования модели безопасности для данной конкретной информационной системы;
- **Системы обнаружения атак** — устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности;
- **Резервное копирование** — сохранение избыточных копий информационных ресурсов на случай их возможной утраты или повреждения;
- **Дублирование (резервирование)** — создание альтернативных устройств, необходимых для функционирования информационной среды, предназначенных для случаев выхода из строя основных устройств;

- **Аварийный план** — набор мероприятий, предназначенных для претворения в жизнь, в случае если события происходят или произошли не так, как было предопределено правилами информационной безопасности;

  Обучение пользователей — подготовка активных участников информационной среды для работы в условиях соответствия требованиям информационной безопасности.

Основные направления информационной безопасности:

1. **Физическая безопасность** — обеспечение сохранности самого оборудования, предназначенного для функционирования информационной среды, контроль доступа людей к этому оборудованию. Дополнительно сюда может быть включено понятие защиты самих пользователей информационной среды от физического воздействия злоумышленников, а также защиты информации не виртуального характера (твердых копий — распечаток, служебных телефонных справочников, домашних адресов сотрудников, испорченных внешних носителей и т. п.).

2.Компьютерная безопасность (сетевая безопасность, телекоммуникационная безопасность, безопасность данных) — обеспечение защиты информации в ее виртуальном виде. Возможно выделять этапы нахождения информации в среде, и по этим принципам разделять, например, компьютерную (на месте создания, сохранения или обработки информации) и сетевую (при пересылке) безопасность, но это, в принципе, нарушает комплексную картину безопасности. Единственное, с чем логично было бы согласиться, — это термин безопасность данных, или скорее, безопасность данных в рамках данного приложения. Дело в том, что в конкретном программном комплексе модель безопасности может быть реализована таким образом, что это потребует отдельного специалиста (или даже службы) по ее поддержанию. В этом случае возможно разделить понятия безопасность данных (конкретного приложения) и безопасность сети (всей остальной информационной среды).

Терминология

- **Субъектом** — пользователя информации или процесс, обрабатывающий данный набор информации (объект) и учитываемый, применительно к данному рассмотрению, в момент того или иного использования объекта.
  Следовательно, **объект** — это некий пассивный, а **субъект** — активный участник процесса обмена информацией.
  Информационная система — это некий потенциально открытый набор субъектов, воздействующих на набор объектов, причем субъекты одной системы обычно имеют общую цель или цели.
  Информационное пространство — это совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь иные, в том числе прямо противоположные, интересы, чем другая.
  Правила информационной безопасности — список разрешенных и/или запрещенных действий для субъектов информационной системы. Такие правила могут быть определены не только для человека (пользователя, администратора и т. д.), но и для процесса (например, процесса предоставления доступа на межсетевом экране).

- **Права** (англ. rights) — набор разрешенных действий (правил) для данного субъекта, часть профиля субъекта.

  Несанкционированным будем считать такое действие, которое производится субъектом (или частью субъекта), для которого данное действие не определено как разрешенное (либо определено как запрещенное) правилами информационной безопасности.

  Средство работы с информацией — устройство информационного обеспечения, с помощью которого производится или обеспечивается работа в информационной системе.

  Угроза — возможность реализации нарушения того или иного правила информационной безопасности.

  Уязвимость (англ. vulnerability) — незащищенность или ошибка в объекте или информационной системе, которая приводит или может привести к возникновению угрозы.

- **Атака** — практическая реализация угрозы или попытка ее реализации с использованием той или иной уязвимости.
  Авария — незлоумышленное происшествие неординарного характера, несущее деструктивное воздействие на объект или информационную систему.
  Пользователь — человек, субъект информационной системы, выполняющий в ней бизнес-функции, т. е. использующий объект в целях производства.
  Администратор — человек, субъект информационной системы, создающий условия для работы в ней пользователей.

Еще не много терминологии

- **Контролер** — субъект (не обязательно человек!) информационной системы, контролирующий использование информационной системы пользователями и администраторами в соответствии с предопределенными правилами (правилами информационной безопасности).

  Злоумышленник — человек, субъект информационной системы, преследующий корыстные или деструктивные цели, противоречащие бизнес-целям системы.

  Идентификатор (имя, логин) — набор символов, представляющий уникальное наименование данного объекта или субъекта в данной (в другой системе имя может повториться) информационной системе. Позволяет однозначно идентифицировать пользователя при входе его в систему, определить его права в ней, фиксировать действия и т. п.

- **Пароль** (англ. password) — секретная последовательность символов, связанная с субъектом и известная только ему, позволяющая его аутентифицировать, т. е. подтвердить соответствие реальной сущности субъекта предъявляемому им при входе идентификатору. Профиль (англ. profde) — набор установок и конфигураций, специфичный для данного субъекта или объекта и определяющий его работу в информационной системе.

Шифрование (англ. encryption) — процесс приведения информации в форму, при которой невозможно или существенно затруднено извлечение из нее осмысленных данных без обладания специфическими дополнительными знаниями (ключом).

Дешифрование (расшифрование) (англ. decryption) — процесс, обратный процессу шифрования, т. е. восстановление с помощью соответствующего ключа информации в исходной форме, позволяющей извлечь из нее смысловые данные.

Криптоанализ — набор методов и средств для выполнения (или сам процесс) дешифрования информации без обладания необходимым ключом.

- **Электронный документ** — набор данных в электронном представлении, который может быть путем стандартных преобразований представлен в понятном человеку виде, в том числе как документ на бумаге; является неделимой единицей обмена информацией, т. е. он может быть передан (получен) либо не передан (не получен) только целиком; состоит из элементов, называемых реквизитами документа.

  Закрытый ключ (приватный ключ, секретный ключ) — секретная последовательность байт, предназначенная для формирования субъектом электронной цифровой подписи для электронных документов.

  Открытый ключ (публичный ключ) — последовательность байт, связанная с закрытым ключом и предназначенная для проверки электронно-цифровой подписи у электронных документов. Открытый ключ должен быть в распоряжении проверяющей стороны.

Задачи службы информационной безопасности

- Существует ряд рекомендаций по вопросам размещения, взаимодействия и подчинения службы безопасности, как продвинутые, в основном западные, ориентированные на электронный мир, так и старые, еще советские, пришедшие от первых отдело, эти процедуры очень зависят от множества факторов конкретного предприятия, быть может даже таких, как сложившиеся неформальные взаимоотношения между сотрудниками. Если во главу угла на предприятии ставится эффективность работы службы информационной безопасности, то такие аспекты невозможно не учитывать.
  Чтобы не очерчивать жестких рамок для всего этого, предлагаем просто рассмотреть проблемы и ответить для себя на возникающие вопросы. Из полученных ответов станет ясно, как и где должна располагаться служба информационной безопасности на организационном дереве предприятия.

Чем должна заниматься служба безопасности

1. Администрировать имеющиеся средства безопасности (межсетевые экраны, антивирусные пакеты, системы обнаружения атак и пр.)
2. Разрабатывать модели и схемы защиты информации, принимать решения о приобретении новых средств безопасности
3. Контролировать работу пользователей информационного пространства предприятия

Сфера охвата информационных систем

- Функции данной информационной системы, с одной стороны, достаточно специфичны и требуют серьезной подготовки для ее администрирования и/или контроля, а, с другой стороны, слишком незначительны в рамках предприятия для того, чтобы содержать (обучать) двух администраторов для ее контроля. Информационная система имеет вид "черного ящика": все работы по ее администрированию выполняются внешним провайдером, который не может допустить посторонних к этому процессу.

Сфера охвата персонала

- Еще один важный вопрос, возникающий в связи с персоналом организации, — это осведомленность службы безопасности о текущем статусе каждого из работников. В идеале служба безопасности должна принимать участие в приеме на работу (если не в принятии решения о приеме, то в инструктаже по нормативным документам и правилам), увольнении с должности (подписании обходного листа), а также периодически получать информацию об отпусках (в частности, знать все о путешествиях сотрудников), командировках, болезнях и прочих данных, очевидно, на сколько важна профилактика гриппа и простуды.

Сфера охвата проектов

- Таким образом, мы рассмотрели ряд проблем, с которыми можно столкнуться в процессе формирования или реформирования службы информационной безопасности. Скорее всего в каждом конкретном случае в этот список добавится еще большое число вопросов, специфичных для данного предприятия. От их решения зависят и принципы формирования службы. При этом следует помнить, что каждая новая задача, возложенная на службу безопасности, потребует, как и в любом другом случае, дополнительных людских ресурсов, расходов на обучение, других операционных расходов.

Контроль функционирования службы

- **Шаг 1.** Привязать ИТ-проекты к целям и задачам предприятия Эффективное измерение вклада ИТ в общие достижения предприятия начинается на стадии планирования и основывается на главной задаче организации и стратегическом бизнес-плане. Связь ИТ-проектов с целями и задачами предприятия может быть установлена с помощью норматива "Сбалансированный учет" (Balanced Scorecard), состоящего из четырех направлений: финансового, работы с заказчиком, внутреннего производства, инноваций и обучения.
  Шаг 2. Разработать средство измерения производительности Выбирается ограниченный набор значимых мер по кратко- и долгосрочным целям. Результаты ИТ-инвестиций выражаются не только в стоимости, своевременности и качестве. Результат — это эффект, который оказали ИТ-инвестиции на организацию. Примерами могут служить измеряемые улучшения в качестве и в доставке продуктов и услуг организации до клиента. Для конкретизации мер надо определить задачи проекта, решить, за счет чего будет достигаться выполнение требований, знать, как влияет результат на последующее развитие. Эффективность их обычно отражает сфокусирование на клиенте.

- **Шаг 3.** Установить основу для сравнения с изменением производительности в будущем
  Данная основа должна определить, улучшилась или ухудшилась производительность в результате вложений в ИТ. Эта основа должна быть задокументирована, рассмотрена и утверждена заказчиками и организаторами работ. Обычные отчеты могут служить основой, если они соотнесены с предопределенным индикатором производительности.
  Шаг 4. Выбрать наиболее значимые ИТ-проекты
  Поскольку организация может финансировать ограниченное число ИТ-проектов, надо выбрать те, которые наиболее значимы. Выбор основывается на оцениваемой экономической прибыли от ИТ-инвестиций плюс предполагаемый вклад в бизнес-приоритеты организации. Для оценки значимости и риска каждого вложения создается Совет по анализу инвестиций (Investment Review Board).

- **Шаг 5.** Собирать данные
  На шагах 2 и 3 необходимо задуматься, какие данные необходимы для определения результата и эффективности проекта. Выбор пакета данных зависит от того, что имеется в распоряжении, от затрат на их получение и актуальности их значений.
- **Шаг 6.** Анализировать результаты
  После того как результаты получены, необходимо их рассмотреть, чтобы определить, соответствует ли выполнение проекта задачам и адекватно ли индикаторы отражают результаты. Основной вопрос в том, отличаются ли результаты от того, что ожидалось. Во время анализа необходимо производить поиск способов для улучшения производительности, уточнения индикаторов и приобретения опыта. Хороший отчет о производительности отслеживает результат во времени и определяет тенденции.

- **Шаг 7.** Объединяться с процессом управления
  Для того чтобы быть уверенным, что результаты улучшают производительность, необходимо оценивать их с точки зрения текущего процесса управления. Ведь если результаты не будут использоваться предприятием, то и процесс их измерения не нужен. Если выполнение проекта растянуто на несколько лет, то определять результаты нужно ежегодно.
- **Шаг 8.** Сообщать о результатах
  Необходимо информировать работников и руководителей о результатах внутри предприятия для улучшения координированности и целеустремленности. Если требуется поддержка и дополнительное финансирование проекта, то о результатах надо сообщать в вышестоящие инстанции. Для укрепления партнерских отношений о результатах информируют клиентов.

Создание службы безопасности

- Нужна или не нужна служба информационной безопасности? Как определить время, когда необходимо ответить на этот вопрос положительно (если такая служба еще не создана)? Это зависит от множества причин и условий, но первая стадия может определяться исходя из комбинации следующих пунктов:
  - в вашей организации уже больше 10 компьютеров, распределенных по различным помещениям;
  - в вашей организации создана локальная сеть;
  - один из компьютеров вашей организации соединен с модемом;
  - вы храните/обрабатываете на компьютере информацию, разглашение или утеря которой может принести вашей организации существенный ущерб.

Состав службы информационной безопасности

- **Сотрудником службы безопасности должен быть достаточно подготовленный специалист, так как ему необходимо следующее:**
  1. Разбираться в общих чертах в технических особенностях используемого информационного обеспечения (включая аппаратное и программное обеспечение, принятые де-юре и де-факто методы работы в информационном пространстве организации и т. п.). Иначе он просто не будет понимать, чем занимаются его подчиненные, а те в свою очередь смогут манипулировать своим руководителем.
  2. Осуществлять надзорные функции как формализованные, так и нет, в том числе управление проектами, так как внедрение многих механизмов безопасности (например, таких как приобретение и внедрение технических решений) потребует проектной работы.
  3. Разбираться в психологии работников, уметь разрешать конфликты (так как служба безопасности часто сама служит основой для репрессивного или ограничительного воздействия). Возможно, придется использовать слабые или сильные стороны различных сотрудников организации.

- 4. Знать основы существующего законодательства, так как, возможно, придется производить расследования, в которых будут фигурировать такие понятия, как "право частной собственности на информацию", "улики и доказательства", "свидетельства" и т. п.
  5. Налаживать связи как с коллегами в других организациях, так и с вышестоящими организациями для защиты интересов своей компании в соответствующей сфере.
  6. Пользоваться доверием руководства, так как при определенном желании можно создать такую ситуацию, когда на службу безопасности будет замкнуто очень многое, что даст возможность ее руководителю использовать свой пост в личных интересах.

Уровень подготовки специалистов

- Существует специальная организация International Information Systems Security Certification Consortium, Inc. (Международный консорциум по сертификации в области информационной безопасности), которая занимается тестированием и сертификацией специалистов по информационной безопасности, а CISSP — это ни что иное, как Certified Information Systems Security Professional (Сертифицированный специалист в области информационной безопасности). Другая категория, по которой проводится сертификация, — это SSCP — Systems Security Certified Practitioner (Сертифицированный практикующий специалист по безопасности систем).

Законодательство

Защита конфиденциальной информации в РФ регулируется следующими федеральными законами:

1. №160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19 декабря 2005 г.
2. №152-ФЗ «О персональных данных» от 27 июля 2006 г.
3. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.
4. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» по вопросам международных договоров Российской Федерации о реадмиссии »от 25 ноября 2009 г.

- *Спасибо за внимание!*