Основы системы обеспечения информационной безопасности

Вводная часть

В ходе данного занятия будет рассмотрено понятие «системы обеспечения информационной безопасности» и ее содержание.

Актуальность данного занятия определена растущим уровнем угроз, рисков для предприятий и организаций любого типа, что приводит к необходимости искать современные методы защиты информации, позволяющие системно решить задачу обеспечения информационной безопасности.

С конца 2018 года Правительством Российской Федерации разрабатывается Концепция суверенного Рунета, внедрение которой способно существенно повысить уровень защиты информации. Эта тема привлекает повышенное внимание экспертного сообщества.

Кроме этого, обеспечение безопасности информации требует вложения серьезных финансовых ресурсов. Если компания может позволить себе соизмерять потенциальные расходы, связанные с внедрением современных информационных технологий, с ущербом, который может быть причинен утечкой информации, то государство обязано обеспечить максимально возможную степень защиты. Реализация концепции национального Рунета, импортозамещение в области производства электронной техники и разработки программного обеспечения должны решить задачу обеспечения информационной безопасности в стране.

Поэтому совершенствование системы обеспечения информационной безопасности на предприятиях, фирмах и организациях очень важно в современном мире.

В ходе занятия будет рассмотрен следующий учебный вопрос:

1. Основы системы обеспечения информационной безопасности на предприятии (в организации).

Первый учебный вопрос: «Основы системы обеспечения информационной безопасности на предприятии (в организации)»

В соответствии с Доктриной информационной безопасности Российской Федерации (утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646) система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения,

иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих **принципах**:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

В соответствии с ранее изучаемым **ГОСТ 53114** «Обеспечение информационной безопасности в организации»:

Обеспечение информационной безопасности организации – это деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

Мероприятия обеспечения информационной безопасности – это совокупность действий, направленных на разработку и (или) практическое применение способов и средств обеспечения информационной безопасности.

Критерий обеспечения информационной безопасности организации – это показатель, на основании которого оценивается степень достижения цели (целей) информационной безопасности организации.

Эффективность обеспечения информационной безопасности – это связь между достигнутым результатом и использованными ресурсами для обеспечения заданного уровня информационной безопасности.

Рассмотрим методологию системы обеспечения информационной безопасности.

На предыдущем занятии мы рассмотрели схему информационной безопасности, которая содержит объекты информационной безопасности, силы информационной безопасности и средства информационной безопасности. Кроме этого, для эффективной работы системы информационной безопасности создается система обеспечения информационной безопасности, функционал которой направлен на обеспечение сил и средств информационной безопасности, которые в свою очередь будут обеспечивать надежную защиту конфиденциальной информации (рис. 1).

Рисунок 1 – Система информационной безопасности

В соответствии со схемой, **систему обеспечения информационной безопасности рассмотрим по двум направлениям**:

- обеспечение сил информационной безопасности;
- обеспечение средств информационной безопасности.

Итак, первое направление – **обеспечение сил информационной безопасности**.

Данное направление содержит такие аспекты, как:

- подготовка специалистов информационной безопасности;
- трудоустройство специалистов информационной безопасности;
- обеспечение трудовой деятельности (выполнение функциональных обязанностей) специалистом информационной безопасности;
- увольнение специалиста информационной безопасности или сотрудника, имевшего доступ к конфиденциальной информации или привлекавшегося к выполнению задач информационной безопасности.

Как мы рассмотрели на предыдущих занятиях, к силам информационной безопасности организаций относятся структурные подразделения, выполняющие задачи управления системой информационной безопасности организации.

Поэтому к сотрудникам службы информационной безопасности предъявляется ряд квалификационных требований, которые мы рассмотрим на следующих занятиях. Но данные квалификационные требования формируются у сотрудников не одномоментно, а за определенный промежуток времени – от нескольких месяцев до нескольких лет.

Основными этапами в ***подготовке специалистов информационной безопасности*** являются:

- подготовка специалистов информационной безопасности в учебных образовательных организациях и центрах различного уровня образования

(средне-специального, технического, бакалавриата, специалитета, магистратуры);

- повышение квалификации в зависимости от его базового уровня и занимаемой должности. Повышение квалификации также осуществляется в учебных образовательных организациях и центрах и может осуществляться как с отрывом от производства, так и без отрыва от производства;

- переподготовка специалистов информационной безопасности направлена на получение знаний и умений нового уровня в данной области деятельности. Как правило, переподготовка специалиста осуществляется при его переходе на другую должность.

Для достижения требуемого уровня квалификации разрабатывается ФГОСТ по специальности «Информационная безопасность», а для каждой специализации разрабатываются квалификационные и трудовые требования, т.е. определяется, что должен знать специалист информационной безопасности, что он должен уметь и какими навыками владеть.

Поэтому по окончании обучения проводится итоговая государственная аттестация, выпускники защищают диплом или проект.

При этом необходимо отметить, что в подготовке соответствующего специалиста может быть заинтересовано государство или ведомство, а организация или предприятие может быть заинтересовано в подготовке конкретного сотрудника (или будущего сотрудника).

Как любой вид деятельности подготовка (переподготовка и повышение квалификации) специалистов информационной безопасности обеспечивается:

- нормативно-правовой базой, включая и лицензирование деятельности;

- финансированием подготовки специалистов информационной безопасности;

- обеспечением государственных, муниципальных и других социальных гарантий на период обучения, повышения квалификации и переподготовки специалиста.

Следующий этап в жизни специалиста информационной безопасности – его ***трудоустройство***.

На данном этапе государство, ведомство или организация должны создать и обеспечить наличие рабочих мест формированием отделов или служб информационной безопасности. По окончании обучения, в соответствии с квотами государства или ведомства, выпускники получают рабочие места от «Заказчиков», так же в учебные заведения приезжают представители различных организаций, и в соответствии со своими требованиями отбирают кандидатов на работу в данные организации. Например, в МЭИ есть отдел помощи в трудоустройстве выпускникам, и каждый желающий может подать в этот отдел свои документы. Но вы должны понимать, что успех вашего трудоустройства напрямую будет зависеть от показателей вашей успеваемости, уровня полученных знаний и умений.

Но, к сожалению, в настоящее время вопросы трудоустройства всех выпускников учебных заведений слабо урегулированы, и специалисты, зачастую, самостоятельно занимаются трудоустройством.

При трудоустройстве, как правило, проходит отбор кандидатов. Т.е. проходит собеседование, тестирование или другие способы определения уровня подготовки кандидатов. Соответствующими сотрудниками организации определяются общие и отраслевые требования к специалисту информационной безопасности.

Поэтому трудоустройство также сопровождается нормативно-правовым и финансовым обеспечением, но при этом добавляется кадровое обеспечение.

Следующий этап – ***обеспечение трудовой деятельности*** (выполнение функциональных обязанностей) специалистом информационной безопасности.

Данный этап характеризуется объемом выполняемых обязанностей по информационной безопасности. Но в выполнении задач информационной безопасности участвуют:

- сотрудники службы информационной безопасности;
- руководство организации и начальники различных отделов;
- сотрудники охраны организации;
- сотрудники различных отделов, имеющие доступ к конфиденциальной информации или привлекаемые к выполнению задач информационной безопасности.

Все сотрудники, привлекаемые к выполнению задач информационной безопасности, обеспечиваются должностными обязанностями, договорами и инструкциями, определяющими их функционал.

Кроме этого, указанные сотрудники должны проходить регулярное обучение без отрыва от производства и сдавать зачеты (проверки) по вопросам информационной безопасности. Успешная сдача зачетов и проверок должна стимулироваться руководством организации. При этом, обращаю ваше внимание, все вопросы обучения указанных сотрудников осуществляется службой информационной безопасности.

Все сотрудники организации и, где необходимо, подрядчики и представители третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в организации и необходимых для выполнения их функциональных обязанностей.

Обучение, обеспечивающее доступ к конфиденциальной информации, следует начинать с формального вводного процесса, предназначенного для ознакомления с политиками и ожиданиями организации в области безопасности прежде, чем будет предоставлен доступ к информации или услугам.

Постоянное обучение должно охватывать требования безопасности, правовую ответственность, управление бизнесом, а также обучение правильному использованию средств обработки информации, например, процедуре начала сеанса, использованию пакетов программ и информации об ответственности за нарушение требований по информационной безопасности.

Деятельность, связанная с обеспечением доступа к конфиденциальной информации, обучения и тренинга в отношении безопасности должна быть

адекватной и соответствовать роли, обязанностям и квалификации лица, и должна включать информацию об известных угрозах, о контактном лице для получения дополнительной консультации по безопасности, а также о соответствующих каналах для сообщения об инцидентах информационной безопасности. Обучение с целью повышения уровня доступа к конфиденциальной информации направлено на то, чтобы дать возможность отдельным лицам распознавать проблемы и инциденты информационной безопасности, и реагировать в соответствии с их функциональными обязанностями.

Кроме этого, обучение сотрудников в процессе трудовой деятельности, т.е. без отрыва от производства, может осуществляется в форме так называемого «наставничества», более опытными сотрудниками в данной области.

Поэтому выполнение трудовых обязанностей в области информационной безопасности также сопровождается нормативно-правовым, финансовым, кадровым обеспечением и добавляется организационное обеспечение и аудит информационной безопасности.

Следующий этап – ***увольнение специалиста информационной безопасности или сотрудника, имевшего доступ к конфиденциальной информации или привлекавшегося к выполнению задач информационной безопасности***.

Данный этап характеризуется причинами увольнения:

- увольнение сотрудника на пенсию по достижении соответствующего возраста;

- переход сотрудника в другую организацию или назначение сотрудника на новую должность, функционал которой не требует выполнения работ с конфиденциальной информацией;

- увольнение сотрудника по решению руководителя организации (сокращение штатов, в связи с нарушением требований информационной безопасности или в результате создания сотрудником инцидента информационной безопасности).

Все эти причины определяют режим прекращения доступа увольняемого сотрудника к конфиденциальной информации организации и возложение на него обязательства не разглашать в последующем ту конфиденциальную информацию, к сведениям которой он имел доступ. Данные обязательства подкрепляются договором, в котором могут указываться и возможные ограничения для данного сотрудника по выезду за границу или трудоустройство в конкурирующие организации, а также мероприятиями по контролю за соблюдением настоящего обязательства.

Основными видами обеспечения данного этапа являются нормативно-правовое, организационное, финансовое и кадровое обеспечение организации.

Далее рассмотрим второе направление системы обеспечения информационной безопасности – **обеспечение средств информационной безопасности.**

Как мы рассматривали на предыдущих занятиях, к **средствам обеспечения информационной безопасности** относятся: техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Поэтому средства обеспечения информационной безопасности содержат такие этапы «жизни», как:

- приобретение сертифицированных программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности;
- категорирование программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности;
- установка, настройка, проведение испытаний и ввод в эксплуатацию программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности;
- техническое обслуживание и ремонт программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности в процессе их эксплуатации;
- списание и утилизация программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности, не пригодных для дальнейшей эксплуатации.

Итак, первый этап системы обеспечения средств информационной безопасности – **приобретение сертифицированных программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности**

Важным элементом является сертификация приобретаемых средств. Использование компанией несертифицированной продукции в сфере деятельности, требующей обязательной сертификации средств защиты информации, может повлечь за собой серьезные последствия: от больших штрафов до уголовной ответственности для руководителей.

Сертификация осуществляется ФСТЭК – это процедура получения документа, подтверждающего, что средство защиты информации соответствует требованиям нормативных и методических документов ФСТЭК России.

Сертификация ФСТЭК для средств защиты информации создана для того, чтобы обеспечить:

- защиту конфиденциальной информации строго определенного уровня;
- возможность для потребителей выбирать качественные и эффективные средства защиты информации;
- содействие формированию рынка защищенных информационных технологий и средств их обеспечения.

Поэтому данный этап сопровождается нормативно-правовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **категорирование программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности**

Данный этап регламентирован **приказом ФСТЭК** России от 2 июня 2020 года **№ 76** «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)».

Категорирование – определение уровней доверия для программных и программно-технических средств технической защиты информации, средств обеспечения безопасности информационных технологий, включая защищенные средства обработки информации, характеризующие безопасность применения данных средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа, а также для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Для дифференциации требований по безопасности информации к средствам информационной безопасности устанавливается **6 уровней доверия**. Самый низкий уровень - шестой, самый высокий - первый.

Средства информационной безопасности, соответствующие ***6 уровню доверия***, применяются в значимых объектах критической информационной инфраструктуры 3 категории, в государственных информационных системах 3 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных.

Средства информационной безопасности, соответствующие ***5 уровню доверия***, применяются в значимых объектах критической информационной инфраструктуры 2 категории, в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Средства информационной безопасности, соответствующие ***4 уровню доверия***, применяются в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса.

При проведении сертификации средства защиты информации должно быть подтверждено соответствие средства настоящим Требованиям.

Устанавливается следующее **соответствие классов средств защиты информации и средств вычислительной техники уровням** доверия:

- средства защиты информации 6 класса должны соответствовать 6 уровню доверия;
- средства защиты информации 5 класса должны соответствовать 5 уровню доверия;
- средства защиты информации 4 класса и средства вычислительной техники 5 класса должны соответствовать 4 уровню доверия.

Данные уровни доверия определяются ***наличием возможных уязвимостей*** программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности.

Основой в данном вопросе являются опубликованные в различных источниках сведения о технических уязвимостях. Контроль технических уязвимостей следует осуществлять эффективным, систематическим и повторяемым способом, с проведением измерений с целью подтверждения его эффективности. Эти подходы должны касаться эксплуатируемых систем и любых других используемых прикладных программ.

При этом необходимо получать своевременную информацию о технических уязвимостях используемых средств информационной безопасности, оценивать незащищенность организации в отношении таких уязвимостей и принимать соответствующие меры для рассмотрения, связанного с ними риска. Данная информация позволяет эффективно управлять техническими уязвимостями.

Специальная информация, необходимая для управления техническими уязвимостями, включает в себя информацию о поставщике программного обеспечения, номерах версий, текущем состоянии применяемых средств информационной безопасности (например, какое программное обеспечение установлено на каких системах) и специалистах, отвечающих в организации за программное обеспечение.

Аналогично, своевременное действие должно предприниматься в ответ на выявление потенциальных технических уязвимостей.

Для создания эффективного процесса менеджмента в отношении технических уязвимостей необходимо выполнять следующие мероприятия:

a) в организации необходимо определять и устанавливать роли и обязанности, связанные с менеджментом технических уязвимостей, включая мониторинг уязвимостей, оценку риска проявления уязвимостей, исправление программ, слежение за активами и любые другие координирующие функции;

b) информационные ресурсы, которые будут использоваться для выявления значимых технических уязвимостей и обеспечения осведомленности о них, следует определять для программного обеспечения и другой технологии на основе списка инвентаризации активов; эти информационные ресурсы должны обновляться вслед за изменениями, вносимыми в опись, или, когда найдены другие новые или полезные ресурсы;

c) необходимо определить временные параметры реагирования на уведомления о потенциально значимых технических уязвимостях;

d) после выявления потенциальной технической уязвимости организация должна определить связанные с ней риски и действия, которые необходимо предпринять; такие действия могут включать внесение исправлений в уязвимые системы и (или) применение других мер и средств контроля и управления;

e) в зависимости от того, насколько срочно необходимо рассмотреть техническую уязвимость, предпринимаемое действие следует осуществлять в соответствии с мерами и средствами контроля и управления, связанными с менеджментом изменений, или следуя процедурам реагирования на инциденты информационной безопасности;

f) если имеется возможность установки патча, следует оценить риски, связанные с его установкой (риски, создаваемые уязвимостью, необходимо сравнить с риском установки патча);

g) перед установкой патчи следует тестировать и оценивать для обеспечения уверенности в том, что они являются эффективными и не приводят к побочным эффектам, которые нельзя допускать; если нет возможности установить патч, следует рассмотреть другие меры и средства контроля и управления, например:

1) отключение сервисов, связанных с уязвимостью;
2) адаптацию или добавление средств управления доступом, например, межсетевых экранов на сетевых границах;
3) усиленный мониторинг для обнаружения или предотвращения реальных атак;
4) повышение осведомленности об уязвимостях;

h) в контрольный журнал следует вносить информацию о всех предпринятых процедурах;

i) следует регулярно проводить мониторинг и оценку процесса менеджмента технических уязвимостей в целях обеспечения уверенности в его эффективности и действенности;

j) в первую очередь следует обращать внимание на системы с высоким уровнем риска.

Следующий элемент – ***процесс получения разрешения на использование средств обработки информации***.

При этом необходимо определить и реализовать процесс получения разрешения у руководства на использование новых средств обработки информации.

В отношении процесса получения разрешения следует рассмотреть следующие мероприятия:

a) на новые средства должны быть получены соответствующие разрешения руководства пользователей, утверждающего их цель и использование. Разрешение следует также получать от администратора, ответственного за поддержку среды безопасности локальной

информационной системы, чтобы обеспечить уверенность в том, что все соответствующие требования и политики безопасности соблюдаются;

b) аппаратные средства и программное обеспечение, где необходимо, следует проверять на предмет совместимости с другими компонентами системы;

c) использование персональных или находящихся в частной собственности средств обработки информации, например, ноутбуков, домашних компьютеров или карманных устройств для обработки деловой информации может являться причиной новых уязвимостей, поэтому следует определять и реализовывать необходимые меры и средства контроля и управления. В настоящее время при удаленной работе многих сотрудников данный пункт является очень актуальным.

Таким образом, данный этап также сопровождается нормативно-правовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **установка, настройка, проведение испытаний и ввод в эксплуатацию программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности**.

Эксплуатационные процедуры следует документально оформлять, соблюдать и делать доступными для всех нуждающихся в них пользователей.

Документально оформленные процедуры должны быть подготовлены для действий системы, связанных со средствами обработки информации и связи, таких как процедуры запуска и завершения работы компьютеров (серверов), процедуры резервирования, текущего обслуживания и ремонта оборудования, обращения с носителями информации, управление работой в машинном зале и работы с почтой, а также процедуры обеспечения безопасности.

Данные процедуры должны содержать детальные инструкции по выполнению каждой работы, включая:

a) обработку и управление информацией;

b) резервирование;

c) требования в отношении графика работ, включая взаимозависимости между системами, время начала самой ранней работы и время завершения самой последней работы;

d) инструкции по обработке ошибок или других исключительных ситуаций, которые могли бы возникнуть в процессе выполнения работы, включая ограничения на использование системных утилит;

e) необходимые контакты на случай неожиданных эксплуатационных или технических проблем;

f) специальные инструкции по управлению выводом данных и обращению с носителями информации, например, использование специальной бумаги для печатающих устройств или управление выводом

конфиденциальных данных, включая процедуры по безопасной утилизации выходных данных в случае сбоев в работе;

g) перезапуск системы и соответствующие процедуры восстановления на случай системных сбоев;

h) управление информацией, содержащейся в контрольных записях и системных журналах.

Эксплуатационные процедуры и документально оформленные процедуры действий системы должны рассматриваться как официальные документы, а изменения в них должны санкционироваться руководством. Если технически возможно, менеджмент информационных систем необходимо осуществлять единообразно, используя одни и те же процедуры, инструментальные средства и утилиты.

Эксплуатируемые системы и прикладное программное обеспечение должны быть предметом строгого контроля управления изменениями.

В частности, необходимо рассмотреть следующие аспекты:

a) определение и регистрацию существенных изменений;

b) планирование и тестирование изменений;

c) оценку возможных последствий, включая последствия для безопасности, таких изменений;

d) формализованную процедуру утверждения предполагаемых изменений;

e) подробное информирование об изменениях всех заинтересованных лиц;

f) процедуры возврата в исходный режим, включая процедуры и обязанности в отношении отмены и последующего восстановления в случае неудачных изменений и непредвиденных обстоятельств.

С целью обеспечения уверенности в надлежащем контроле всех изменений в оборудовании, программном обеспечении или процедурах, должна быть формально определена ответственность и разработаны соответствующие процедуры управления. При внесении изменений вся необходимая информация должна сохраняться в контрольном журнале.

Таким образом, данный этап также сопровождается нормативно-правовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **техническое обслуживание и ремонт программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности в процессе их эксплуатации**.

Техническое обслуживание средств информационной безопасности должно проводиться в соответствии с целями обеспечения его непрерывной доступности и целостности.

В отношении технического обслуживания средств информационной безопасности следует рассмотреть следующие мероприятия:

a) оборудование должно обслуживаться в соответствии с рекомендуемыми поставщиком периодичностью и спецификациями;

b) техническое обслуживание и ремонт оборудования должны проводиться только авторизованным персоналом;

c) следует хранить записи обо всех предполагаемых или фактических неисправностях и всех видах профилактического обслуживания;

d) если запланировано техническое обслуживание оборудования, следует принимать соответствующие меры и средства контроля и управления, при этом необходимо учитывать, будет ли техническое обслуживание проводиться персоналом организации или за ее пределами; при необходимости, конфиденциальная информация из оборудования должна быть удалена, или специалисты по техническому обслуживанию и ремонту должны иметь соответствующий допуск;

e) должны соблюдаться все требования, устанавливаемые технической документацией.

Отдельного внимания заслуживает безопасность средств информационной безопасности, находящихся вне помещений организации.

При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, следует учитывать различные риски, связанные с работой вне помещений организации.

Независимо от права собственности использование оборудования для обработки информации вне помещений организации должно быть санкционировано руководством.

Следующие рекомендации необходимо учитывать в отношении защиты оборудования, используемого вне помещений организации:

a) оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах; во время поездок портативные компьютеры нужно перевозить как ручную кладь и по возможности маскировать;

b) необходимо соблюдать инструкции изготовителей по защите оборудования, например, по защите от воздействия сильных электромагнитных полей;

c) для работы вне контролируемой зоны организации следует определить соответствующие меры и средства контроля и управления, исходя из оценки рисков, например, использование запираемых шкафов для хранения документов, соблюдение политики «чистого стола», управление доступом к компьютерам и связь с офисом по защищенным сетям (ИСО/МЭК 18028 «Сетевая Безопасность»);

d) с целью защиты оборудования, используемого вне помещений организации, должно проводиться адекватное страхование, покрывающее указанные риски. Риски безопасности, например, связанные с повреждением, воровством и подслушиванием, могут значительно отличаться для различных объектов и должны учитываться при определении наиболее подходящих мер и средств контроля и управления.

Еще один элемент – ***техническая проверка прикладных программ после изменений эксплуатируемой системы***.

При внесении изменений в эксплуатируемые системы прикладные программы, имеющие большое значение для бизнеса, следует анализировать и тестировать с целью обеспечения уверенности в том, что не оказывается неблагоприятного воздействия на функционирование или безопасность организации.

Этот процесс должен охватывать:

a) анализ мер и средств контроля и управления прикладными программами и процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями эксплуатируемой системы;

b) обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривает анализ и тестирование систем, необходимые при изменениях эксплуатируемой системы;

c) обеспечение уверенности в том, что уведомления об изменениях эксплуатируемой системы поступают своевременно, чтобы дать возможность перед их реализацией провести соответствующие тесты и анализы;

d) обеспечение уверенности в том, что соответствующие изменения вносятся в планы обеспечения непрерывности бизнеса.

Определенной группе лиц или отдельному специалисту следует вменять в обязанность проведение мониторинга уязвимостей, версий патчей поставщиков и их установок.

Следующий элемент – ***ограничения на изменения пакетов программ***.

Необходимо избегать модификаций пакетов программ, ограничиваться необходимыми изменениями и строго контролировать все сделанные изменения.

Насколько возможно и допустимо с практической точки зрения пакеты программ, поставляемые поставщиком, следует использовать без изменений. Там, где необходимо внести изменения в пакет программ, следует учитывать следующее:

a) риск в отношении встроенных мер и средств контроля и управления, и процедур обеспечения целостности;

b) необходимость получения согласия поставщика;

c) возможность получения требуемых изменений от поставщика в качестве стандартной программы обновления;

d) возможные последствия в случае, если организация станет ответственной за будущее сопровождение программного обеспечения в результате внесенных изменений.

Если необходимо внесение изменений, то оригинальное программное обеспечение следует сохранить, а изменения вносить в четко определенную копию. Следует реализовывать процесс управления обновлением программного обеспечения, чтобы иметь уверенность в том, что для всего разрешенного программного обеспечения устанавливаются новейшие одобренные к применению патчи и обновления прикладных программ.

Все изменения необходимо полностью тестировать и документально оформлять таким образом, чтобы их можно было использовать повторно для будущих обновлений программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимой оценочной организацией.

Таким образом, данный этап также сопровождается нормативно-правовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **списание и утилизация программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности, не пригодных для дальнейшей эксплуатации.**

Безопасная утилизация программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности, не пригодных для дальнейшей эксплуатации является не менее важным этапом.

Все компоненты оборудования, содержащие носители данных, следует проверять с целью обеспечения уверенности в том, что любые конфиденциальные данные и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до их утилизации.

Носители данных, содержащие конфиденциальную информацию, необходимо физически уничтожать, или информацию необходимо разрушить, удалить или перезаписать способами, делающими исходную информацию невосстановимой, а не использовать стандартные функции удаления и форматирования.

Поврежденные устройства, содержащие конфиденциальные данные, могут потребовать проведения оценки рисков с целью определения элементов, которые должны быть физически разрушены, направлены на ремонт или списаны.

При этом всегда необходимо помнить, что конфиденциальная информация всегда может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования.

Таким образом, данный этап также сопровождается нормативно-правовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Подводя итог выше изложенному материалу, необходимо отметить, что анализ всех мероприятий системы обеспечения средств информационной безопасности показал, что основными видами обеспечения данного направления являются нормативно-правовое, организационное, финансовое, инженерно-техническое и программно-аппаратное обеспечение организации.

Таким образом возникла необходимость систематизировать информацию о системе обеспечения информационной безопасности, ее составе и функционале.

Система обеспечения информационной безопасности – совокупность правовых, организационных и технических мероприятий, органов, сил, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба собственнику информации.

Данная формулировка определена РЕШЕНИЕМ Совета глав правительств СНГ. «О концепции информационной безопасности государств - участников содружества независимых государств в военной сфере».

Цель СОИБ заключается в обеспечении устойчивого функционирования организации (предприятия) для достижения им своих целей, которое достигается выполнением требований по конфиденциальности, доступности и целостности принадлежащих ему активов.

Задачи СОИБ:

1. Предотвращение угроз безопасности организации (предприятия), защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом РФ, обеспечение стабильной производственной деятельности всех подразделений объекта.

2. Повышение качества предоставляемых услуг и гарантий безопасности.

Для решения этих задач необходимо выполнить следующие **мероприятия СОИБ**:

- отнести информацию к категории ограниченного доступа;
- прогнозировать и своевременно выявлять угрозы безопасности информационным ресурсам, причины и условия, способствующие нанесению финансового, материального и морального ущерба, нарушению нормального функционирования и развития организации;
- создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создать механизм и условия оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических и прочих мер, и средств обеспечения безопасности;
- создать условия для максимально возможного возмещения и (или) локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения информационной безопасности.

Выше изложенные положения определяют **состав системы обеспечения информационной безопасности**:

- подсистема организационно-правового обеспечения;
- подсистема кадрового обеспечения;
- подсистема финансово-экономического обеспечения;
- подсистема инженерно-технического обеспечения;
- подсистема программно-аппаратного обеспечения;

- подсистема аудита информационной безопасности.

Данные подсистемы, представляющие собой единую СОИБ полностью охватывают весь перечень работ по ее созданию в интересах объекта, организации функционирования этой системы и поддержания ее в состоянии готовности к решению возложенных на нее задач.

Подсистема организационно-правового обеспечения должна обеспечить:

- во-первых, формирование правового поля для выполнения мероприятий обеспечения информационной безопасности, путем учета требований законодательства РФ в данной предметной области;

- во-вторых, обеспечение выполнения концептуальных разработок, а также практических ограничительных и режимных мероприятий по обеспечению информационной безопасности в интересах объекта.

При этом, **организационные мероприятия обеспечения информационной безопасности** – мероприятия обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

Таким образом, для обеспечения информационной безопасности организации, создан универсальный перечень режимных (организационных) мероприятий, включающий:

- физическую защиту сотрудников, являющихся потенциальными носителями конфиденциальной информации;

- постоянный контроль и проверка персонала с целью устранения возможностей для совершения мошенничества, предотвращения возможного сговора между сотрудниками и, например, клиентами;

- ограничение прав доступа сотрудников к информации, которое должно регламентироваться только характером выполняемых ими должностных обязанностей;

- налаженную и постоянно действующая система внутреннего контроля, включающая проведение плановых, внезапных и скрытых контрольных проверок;

- проведение предупредительной активной политики аудита информационной безопасности.

Подсистема кадрового обеспечения должна базироваться на созданной системе подготовки специалистов в области информационной безопасности, иметь систему подбора специалистов, основывающуюся на деятельности кадрового органа объекта, а также, систему работы с сотрудниками.

Подсистема финансово-экономического обеспечения обеспечивает выполнение функции использования результатов анализа финансово-экономической деятельности организации с целью определения возможных масштабов финансирования деятельности по обеспечению информационной безопасности.

Кроме этого, обеспечивает работы по моделированию и оценке затрат на обеспечение ИБ, а также, по определению минимально достаточного уровня затрат, т.е. оптимизационные расчеты.

Подсистема инженерно-технического обеспечения охватывает совокупность работ по инженерно-техническому оборудованию элементов (объектов) информационной инфраструктуры организации.

Кроме этого, по обеспечению видеонаблюдения, противопожарной защиты на объектах, и защиты информации, в том числе и компьютерной, от утечек по различным каналам.

Подсистема программно-аппаратного обеспечения обеспечивает выполнение функций защиты информации в информационной системе, а также самих элементов информационной системы от различных угроз применением различных программных и программно-аппаратных решений.

Подсистема аудита информационной безопасности предназначена для обеспечения контроля и проверок качества функционирования всех подсистем и элементов СОИБ применением методик анализа рисков информационной безопасности, а также различных форм проведения проверок.

На этом изложение учебного вопроса завершено.

Литература

1. Доктрина информационной безопасности Российской Федерации (утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)

2. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»

3. ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»

4. ГОСТ 27002-2012 «Методы и средства обеспечения безопасности»

5. Федеральный закон Российской Федерации №149 от 08.07.2006 г. «Об информации, информационных технологиях и о защите информации»

6. Приказ ФСТЭК России от 2 июня 2020 года № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)»

7. ГОСТ ИСО/МЭК 18028 «Сетевая Безопасность»

8. Невский А.Ю., Баронов О.Р. Система обеспечения информационной безопасности хозяйствующего субъекта: учебное пособие. – М.: Издательский дом МЭИ, 2009 г.

Заключение

Из представленного учебного материала вам необходимо уяснить понятие «системы обеспечения информационной безопасности» и ее содержание.

Доцент кафедры БИТ Д.Власкин