системы. Так информационные системы выделяют в зависимости от типа обрабатываемой информации, того, является ли система государственной, имеет ли доступ к открытым каналам данных.

Общий перечень требований включает в себя аудит безопасности, требования по обеспечению защиты данных, требования по обеспечению идентификации и аутентификации, требования по защите системы защиты информации информационной системы, обеспечение криптографической защиты информации, дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре и иные требования.

Требования отличаются в зависимости от типов систем. Так, для некоторых типов систем «обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года» входит в список обязательных требований, а для классов 4-ин, 4-спец, 4-юл, 4-дсп и 3-юл является рекомендуемой частью аудита безопасности.

В ходе аудита составляется акт, в котором каждому вопросу выставляется отметка о выполнении, номер, дата, наименование документа в котором реализованы требования. Обязательным для всех классов систем является этап с составлением требований по обеспечению защиты данных, в рамках которых проводится регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием, и обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности [2].

Список литературы

1. Приказы оперативно-аналитического центра при Президенте Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/law/orders-of-the-oac. – Дата доступа: 07.05.2024.

2. Приказы оперативно-аналитического центра при Президенте Республики Беларусь о технической и криптографической защите персональных данных [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2021-195.pdf. – Дата доступа: 07.05.2024.

ПРОБЛЕМЫ И РЕШЕНИЯ В КОНТЕКСТЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.К. Крамаренко, А.Д. Кулик

Учреждение образования «Брестский государственный технический университет», Брест, Беларусь

ИТ сектор является одним из приоритетных и активно развивающихся как в пределах республики Беларусь, так и за ее пределами. В соответствии с важностью и востребованностью данной области, ставится вопрос о необходимости тщательного подбора и подготовки специалистов в ИТ области, а также защиты информации. Рассматривая эту тему на примере инженеров по информационной безопасности, стоит отметить основные проблемы, связанные с подготовкой специалистов.

1. Недостаток квалифицированных кадров. Быстрое развитие ИТ приводит к дефициту опытных и высококвалифицированных специалистов в области информационной безопасности. Существует значительный разрыв между спросом на таких специалистов и доступностью подготовленных кадров.

2. Обновление учебных программ. Быстрый темп развития технологий требует постоянного обновления учебных программ и материалов, которые используются для подготовки специалистов. Некоторые образовательные учреждения и организации не всегда успевают соответствовать последним требованиям.

3. Необходимость практического опыта. Информационная безопасность – это область, где практический опыт играет важную роль. Однако многие программы обучения не обеспечивают достаточно практических тренировок и опыта работы с реальными системами и уязвимостями. Это может создавать проблемы при вхождении выпускников в профессиональную среду.

4. Быстрое изменение угроз и технологий. Это может привести к устареванию их компетенций и недостаточной готовности к новым угрозам [1].

В целях преодоления данных проблем необходимо соответственно активно развивать и совершенствовать образовательные программы, предоставлять студентам больше практического опыта и обеспечивать доступ к актуальным знаниям и ресурсам. Кроме того, важно содействовать сотрудничеству между образовательными учреждениями, предприятиями и профессиональными организациями для обмена опытом и создания партнерских программ. Инженер по информационной безопасности должен обладать знаниями о различных правовых нормах и регулятивных требованиях. Эти нормы предполагают следующие.

1. Законодательство о защите персональных данных. Инженер по информационной безопасности должен быть ознакомлен с законодательством, регулирующим обработку и защиту персональных данных.

2. Законодательство о кибербезопасности. Инженер по информационной безопасности должен быть знаком с законодательством, касающимся кибербезопасности и защиты информационных систем.

3. Законодательство о киберпреступлениях. Это может включать законы о компьютерных мошенничествах, хакерстве, краже личных данных и других киберпреступлениях.

4. Законодательство о защите интеллектуальной собственности. Инженер по информационной безопасности должен быть ознакомлен с законодательством о защите интеллектуальной собственности, таким как авторские права, патенты, товарные знаки и другие права интеллектуальной собственности. Беларусь участвует в двусторонних международных договорах по вопросам интеллектуальной собственности [2].

Требования к знанию правовых норм могут также различаться в зависимости от конкретной страны или региона, а потому в конкретных случаях требуют уточнения и заверения. Поэтому инженер по информационной безопасности должен следить за обновлениями и изменениями в законодательстве, связанном с информационной безопасностью в своей конкретной области работы.

Список литературы

1. Черноокий, И. В. Тенденции внедрения ИТ в образовательный процесс высшей школы в Республике Беларусь / И. В. Черноокий // Проблемы устойчивого развития регионов Республики Беларусь и сопредельных стран : сборник научных статей XI Международной научно-практической интернет-конференции, Могилев, 1–30 июня 2022 г.; под ред. Н. В . Маковской. – Могилев : МГУ имени А. А. Кулешова, 2022. – С. 111–114.

2. Интеллектуальная собственность [Электронный ресурс] – Режим доступа: https://president.gov.by/ru/belarus/science/intellectual-property. – Дата доступа: 06.05.2024.