МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 05 03 Информационные системы и технологии Направление специальности 1-40 01 05 03 Информационные системы и технологии

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №1:**

по дисциплине «Защита и надёжность информационных систем»

Тема «Разработка и внедрение политики безопасности организации или учреждения. Учреждение образования. Детский сад»

Исполнитель

студентка 3 курса группы 1 Кашперко Василиса Сергеевна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Цель: приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения.

Ход работы

*1. Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении).*

Политика информационной безопасности определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется учреждение образования – детский сад в своей деятельности.

Основными целями политики информационной безопасности являются защита информации учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности.

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Задачами настоящей политики являются:

* описание организации системы управления информационной безопасностью;
* определение Политик информационной безопасности, а именно:
* политика реализации антивирусной защиты;
* политика учетных записей;
* политика предоставления доступа к информационному ресурсу;
* политика использования информационного ресурса в рамках существующих информационных систем;
* политика использования паролей;
* политика защиты АРМ;
* политика конфиденциального делопроизводства;
* определение порядка сопровождения ИС.

*2. Объекты защиты. Описание структуры организации (учреждения), периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.*

Настоящая Политика распространяется на все структурные подразделения и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого.

Структура управления определяется также как форма разделения и кооперации управленческой деятельности.

Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Опишем структуру дошкольного учебного учреждения «Детский сад»:

* Заведующая
  + Главный бухгалтер

Бухгалтерия

* + Заместитель заведующей по экономике и финансам

Планово-экономический отдел

Финансовый отдел

Отдел труда и заработной платы

* Заместитель заведующей по учебно-воспитательной работе
* Заместитель заведующей по организационным вопросам
* Заместитель заведующей по административно-хозяйственным вопросам
* Администратор информационной безопасности

В системе управления ИБ должны быть реализованы следующие процессы:

− разработка плана обработки рисков ИБ;

− реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;

− реализация программ по обучению и осведомленности ИБ;

− обнаружение и реагирование на инциденты безопасности;

− обеспечение непрерывности деятельности и восстановления после прерываний.

Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

Ответственность за реализацию политик возлагается:

− в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на администратора информационной безопасности;

− в части, касающейся доведения правил политик до сотрудников, а также иных лиц – на администратора информационной безопасности;

− в части, касающейся исполнения правил политики;

– на каждого сотрудника, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

*3. Основные угрозы и их источники. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.*

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

− показателей ценности информационных ресурсов;

− вероятности реализации угроз для ресурсов;

− эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности организации.

Все многообразие потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

Искусственные угрозы – это угрозы, вызванные деятельностью человека.

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними (о чем мы вспоминали выше).

Основные источники угроз безопасности информации можно классифицировать следующим образом:

• непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей ИВС (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов ИВС;

• преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы:

− деятельность преступных групп и формирований, политических и экономических структур, разведок иностранных государств, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности ИВС в целом и ее отдельных компонентов;

− удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних информационно-телекоммуникационных сетей общего пользования (прежде всего сеть Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена,

средств защиты и разграничения удаленного доступа к ресурсам;

• ошибки, допущенные при разработке компонентов информационной системы и системы ее защиты, ошибки в программном

обеспечении, отказы и сбои технических средств (в том числе

средств защиты информации и контроля эффективности защиты).

В связи с этим, наиболее возможными видами угроз являются следующие:

* «фишинг» по электронной почте;
* вирусы, принесенные в почтовых файлах или USB-носителях;
* угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;
* получение несанкционированного доступа к веб-сайту сайта детского сада. Данный тип атаки наименее опасен, поскольку у сайта так же нету связи с финансовой системой сети. Однако злоумышленники могут испортить информацию на веб-сайте и благодаря этому извлечь какую-нибудь выгоду, либо осуществить «взлом» просто ради интереса;
* атака на детский сад. Данная угроза очень опасна прежде всего риском жертв среди сотрудников. При осуществлении данной атаки, преступники могут завладеть финансами и/или банковскими данными;
* взлом банковского счета детского сада. В настоящее время у любого учреждения имеется свой счет, на котором находятся деньги. Естественно, данная угроза наименее зависима от самого учреждения, так как атака осуществляется на банк. Тем не менее, компания должна предусмотреть данный случай и минимизировать его возможность;
* недобросовестная конкуренция. Данная угроза так же присутствует всегда у любой компании, независимо от ее размера, поэтому ей необходимо уделить внимание при разработке политики информационной безопасности;

Ответственными за реализацию таких мер являются, безусловно, сотрудники системы безопасности компании, наравне с сотрудниками IT-отдела, которые отвечают за информационную безопасность.

*4. Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты.*

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

− привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

− возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

− техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;

− степенью легкости, с которой уязвимость может быть использована.

Таблица 1. Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (ущерб x вероятность) |
| Спам (переполнение почтового ящика\_ | 1 | 0,4 | 0,4 |
| «Фишинг» | 3 | 0,3 | 0,9 |
| Вирусы, перенесенные на компьютеры | 4 | 0,2 | 0,8 |
| Взлом банковского счета | 4 | 0,1 | 0,4 |
| Получение несанкционированного доступа к веб-сайту | 3 | 0,2 | 0,6 |
| Недобросовестная конкуренция | 2 | 0,2 | 0,4 |
| Атака на детский сад и причинение материального и морального ущербов | 5 | 0,11 | 0,55 |
| ЧС природного и техногенного характера | 4 | 0,2 | 0,8 |
| ИТОГО: |  |  | 4,85 |

*5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения).*

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на детский сад, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* охрана детского сада;
* четкая и строгая иерархия должностей и полномочий. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого работника с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита важной корпоративной почты;
* защита личных документов, отчетов в бумажном виде – копирование и перенесение информации на электронные информационные носители, защита помещения, хранящего докумнеты;
* использование новейших средств защиты (антивирусные продукты, firewalls, brandmauer) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие в детском саду наглядного отображения плана по работе во время чрезвычайных ситуаций.

*Выводы и предложения*

В ходе выполнения лабораторной работы я приобрела практические навыки разработки и внедрения эффективной политики информационной безопасности организации или учреждения.