**Лабораторная работа № 1**

## РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ИЛИ УЧРЕЖДЕНИЯ

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

**Теоретические сведения**

**ПИБ** – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками в своей деятельности.

**ИС(ИВС)** – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (ИВ) процессы.

**Информационные процессы** – процессы сбора, накопления, хранения, обработки, передачи и использования информации.

**Информационные ресурсы** – отдельные документы или массивы документов в информационных системах.

**Объект** – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию.

**Субъект** – активный компонент системы, который может инициировать поток информации.

**Доступ** – тип взаимодействия между объектом и субъектом, в результате – поток информации от одного к другому.

**Атака** – попытка несанкционированного преодоления защиты системы.

**Несанкционированный доступ (НСД)** – доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома владельца и нарушающий тем самым установленные правила доступа.

**Защита информации** – организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

**Безопасность информации** – защищенность информации от нежелательного ее разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Безопасность любого ресурса информационной системы складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности (CIA):

* **конфиденциальность** (англ. confidentiality) компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия;
* **целостность** (англ. integrity) компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права; целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени;
* **доступность** (англ. availability) компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Для создания эффективной системы информационной безопасности организации или учреждения целесообразно разработать: *концепцию, стандарты, процедуры, инструкции, план мероприятий, аварийные планы.*

**Разделы концепции ИБ:**

* определение ИБ (или СУИБ);
* структура информационной системы организации (учреждения) и вытекающая из этого структура системы обеспечения информационной безопасности;
* безопасность информации: принципы и стандарты;
* оценка рисков информационным ресурсам в организации (учреждении);
* обязанности и ответственность каждого отдела, управления или департамента, каждого сотрудника в реализации разработанной и утвержденной политики безопасности;
* обязанности лица (администратора безопасности), ответственного за организацию оперативного контроля и управления политикой безопасности;
* ссылки на документы об информационной безопасности, действующие на территории Республики Беларусь.

**Фактор, воздействующий на ИВС** – это явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение данных, блокировка доступа к ним, повреждение или уничтожение системы защиты.

**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.

**Цель оценивания рисков** состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

ПИБ должна рассматриваться как *система*, как комплекс инструментов по защите информации.

**Практическое задание**

1. Цели и задачи

Увеличение числа кибератак и утечек данных подтверждает необходимость разработки и реализации эффективных мер защиты информации в учреждениях. Многие угрозы могут не только нанести ущерб репутации учреждения, но и привести к финансовым потерям и юридическим последствиям. В связи с этим, актуальность информационной безопасности становится очевидной, требуя постоянного мониторинга, анализа и обновления стратегий защиты.

Основной целью является обеспечение информационной безопасности учреждения. Это предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации. Важным аспектом является адекватное отражение угроз информационной безопасности, которое должно быть подчинено единой стратегии.

Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

* документирование требований ИБ;
* выявление, прогнозирование и оценка рисков и угроз;
* создание механизма оперативного реагирования на угрозы ИБ;
* предотвращение и/или снижение до приемлемого уровня ущерба от реализации актуальных угроз;
* недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
* соблюдение законодательных, нормативных и договорных требований в области ИБ;
* реагирование на инциденты ИБ;
* контроль состояния ИБ;
* повышение осведомленности в вопросах обеспечения ИБ;
* постоянное совершенствование систем обеспечения ИБ;
* выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников.

1. Субъекты и объекты информационной безопасности

Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его сотрудниками и должностными лицами.

Настоящая политика распространяется на информационные системы учреждения.

Объектами защиты в Компании являются информация, обрабатываемая в Компании, вне зависимости от формы представления, включая, но не ограничиваясь следующим перечнем:

* автоматизированные рабочие места, средства обработки информации и мобильные технические средства;
* информационные ресурсы ограниченного распространения, в том числе содержащие конфиденциальные сведения;
* программные информационные ресурсы, а именно: прикладное, программное, обеспечение, системное программное обеспечение, инструментальные средства и утилиты;
* носители информации всех видов (электронные, бумажные и прочие);
* ИС, системы хранения данных, программное обеспечение и отдельные технические решения;
* ИТ-инфраструктура, информационно-телекоммуникационные сети и системы связи;
* ИТ-сервисы (ИТ-услуги), оказываемые Компании или в интересах Компании;
* все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением.

Субъектами информационной безопасности являются:

ответственные за ИБ в ИС – должностные лица или структурные подразделения, обеспечивающие ИБ в той или иной ИС;

ответственное подразделение по защите сетевой и вычислительной инфраструктуры – структурное подразделение, организующее разработку, внедрение и функционирование технической системы ИБ, имеющее в составе специалистов, выполняющих функции администратора ИБ ИС;

ответственное лицо по структурному подразделению – работник Компании, назначаемый руководителем структурного подразделения согласно приказу;

пользователи ИС – работники, клиенты, сотрудники Компании, использующие ИС для решения задач.

1. Основные угрозы и их источники

Основные угрозы информационным активам Компании включают в себя:

* разглашение защищаемой информации;
* компрометацию ключевой информации, персональных идентификаторов, паролей;
* несанкционированный доступ к защищаемой информации Компании;
* ввод некорректных (ложных) данных в ИС Компании;
* выход из строя материальных носителей защищаемой информации;
* уничтожение (утеря) защищаемой информации;
* вирусное заражение;
* несанкционированное или некорректное внесение изменений в информационные системы Компании;
* несанкционированное делегирование полномочий и/или использование привилегий;
* угрозы нарушения целостности и функционирования Компании в целом.

Источники угроз ИБ делятся на три основных класса:

* источники, связанные с действиями людей – внешние и внутренние нарушители;
* источники, связанные с природными явлениями (стихийными бедствиями) и деятельности человека – естественные и искусственные;
* источники, вызванные преднамеренно или непреднамеренно.

В качестве внешних нарушителей ИБ рассматриваются лица, не входящие в состав пользователей и обслуживающего персонала ИС Компании, например, разработчики ИС, внешние лица (хакеры, члены криминальных организаций, бывшие работники Компании и т.п.).

В качестве потенциальных внутренних нарушителей ИБ рассматриваются пользователи и обслуживающий персонал ИС Компании, другие субъекты (лица), вовлеченные в информационные процессы Компании, которые также имеют возможность санкционированного доступа к ИС и информационным активам Компании.

Непреднамеренные нарушения (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) устанавливают регламенты сбора, обработки и передачи информации, а также требования информационной безопасности.

Преднамеренные действия (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) могут исходить от работников, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения информационной безопасности.

1. Оценка угроз, рисков и уязвимостей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Угроза | Средства защиты | Ущерб | Вероя  тность | Риск |
| Кражи, нападения, взлом, саботаж и проникновение | Наличие охраны;  Наличие системы видеонаблюдения;  Наличие пропускной системы с удостоверением личности для рабочего персонала. | 4 | 0,1 | 0,3 |
| Фарминг (перенаправление на фейковый IP-адрес) | Использовать защиту электронного почтового ящика (отключить предварительный просмотр);  Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов. | 1 | 0,2 | 0,2 |
| Mailbombing | Давать адрес электронной почты только проверенным источникам. | 2 | 0,3 | 0,6 |
| Копирование архивных данных | Больше внимания уделить защите этих данных | 3 | 0.1 | 0.3 |
| Фишинг/смишинг | Использовать только проверенные ресурсы и пути доступа к ним. | 4 | 0,3 | 1,2 |

1. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

* средства обработки информации, поддерживающие критически важные и уязвимые ресурсы, должны быть размещены в защищённых областях;
* защищённые области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающими возможность доступа только авторизованного персонала;
* места доступа, через которые неавторизованные лица могут попасть в помещения, должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа;
* все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Учреждения;
  + со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО;
* предоставление паролей должно контролироваться посредством официальной процедуры;
* должны быть реализованы меры защиты от вредоносного программного обеспечения (вредоносного кода) для всех компонентов информационной инфраструктуры;
* в целях защиты конфиденциальной информации в Компании могут применяться средства криптографической защиты информации;
* должны осуществляться регулярный мониторинг и регистрация системных событий, действий пользователей и администраторов, ошибок и событий ИБ;
* должен быть организован процесс управления уязвимостями, включающий в себя постоянное выявление, анализ и устранение выявленных уязвимостей;
* должен быть организован процесс управления инцидентами ИБ, в рамках которого каждый инцидент ИБ должен фиксироваться и расследоваться.

1. Вывод

Составление политики безопасности позволяет установить четкие стандарты и процедуры для защиты информации, что способствует системному подходу к управлению рисками и повышению уровня безопасности в организации. Хорошо разработанная политика безопасности не только помогает предотвращать инциденты, но и минимизирует последствия в случае их возникновения, что в конечном итоге экономит ресурсы и защищает репутацию организации. Дополнительно, такая политика может помочь в соблюдении законодательных и нормативных требований, что снижает риск юридических последствий и штрафов. Политика безопасности является основой для создания системы реагирования на инциденты, позволяющей организации быстро и эффективно справляться с угрозами и минимизировать ущерб.