Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ

УНИВЕРСИТЕТ»

**Отчёт**

по предмету «Защита информации и надёжность информационных систем»

Лабораторная работа №1

«Разработка и внедрение политики безопасности организации или учреждения»

Студент: Стрелковская В.А.

ФИТ 3 курс 2 группа

Преподаватель: Хартанович А.А.

1. **Теоретические сведения**

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

**Политика информационной безопасность (ПИБ)** организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

**Информационная (информационно-вычислительная) система** – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

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

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

**Объект** – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

**Субъект** – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

**Доступ** – специальный тип взаимодействия между объектом и субъектом, в результате которого создается 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 (санкции) 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 (для соответствующих субъектов информационных

отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), 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, также могут быть включены другие, такие как аутентичность, подотчетность, надежность; или иначе: информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки:

* 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 информационной безопасности, которая определяет в целом цели политики и основные ее принципы в увязке со статусом, целями и задачами организации или учреждения;

• стандарты (менеджмента качества) – правила и принципы защиты информации по каждому конкретному направлению деятельности;

• процедуры – описание конкретных действий по защите информации при работе с ней: персональных данных, порядка доступа к нформационным носителям, системам и ресурсам;

• инструкции, содержащие подробное описание (алгоритмы) действий по организации информационной защиты и обеспечению разработанных стандартов и процедур;

• план мероприятий по обучению персонала и тестированию знаний сотрудников, имеющих доступ к информационным ресурсам.

Все вышеуказанные элементы должны быть взаимосвязанными и непротиворечивыми.

Для эффективной организации системы информационной безопасности целесообразно разработать аварийные планы. Они необходимы на случай восстановления информационных систем при возникновении форс-мажорных обстоятельств: аварий, катастроф и т. д.

Обеспечение ИБ на предприятиях и в учреждениях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач.

Основными разделами концепции информационной безопасности могут быть следующие:

* 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);
* описание основных механизмов контроля безопасности;
* 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. Все многообразие дестабилизирующих факторов можно разделить на два класса: внутренние и внешние.

*Внутренние дестабилизирующие факторы влияют:*

1. на программные средства (ПС):

* некорректный исходный алгоритм;
* неправильно запрограммированный исходный алгоритм (первичные ошибки);

1. на аппаратные средства (АС):

* системные ошибки при постановке задачи проектирования;
* отклонения от технологии изготовления комплектующих изделий и АС в целом;
* нарушение режима эксплуатации, вызванное внутренним состоянием АС.

*Внешние дестабилизирующие факторы влияют:*

1. на программные средства:

* неквалифицированные пользователи;
* несанкционированный доступ к ПС с целью модификации кода;

1. на аппаратные средства:

* внешние климатические условия;
* электромагнитные и ионизирующие помехи;
* перебои в электроснабжении;
* недостаточная квалификация обслуживающего персонала.

**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.**

1. **Практическое задание**

**2.1 Обоснование актуальности, цели и задачи разработки ПИБ**

Логистические компании ежедневно обрабатывают огромные массивы информации, включая конфиденциальные данные клиентов, сведения о маршрутах, складах, финансовых операциях и технической инфраструктуре. Современные цифровые технологии существенно облегчают управление этими процессами, но вместе с тем увеличивают риски, связанные с возможными кибератаками, утечками данных и техническими сбоями. Важно понимать, что в условиях высокой конкуренции и глобализации логистический бизнес сталкивается не только с внутренними угрозами, такими как ошибки персонала или недостаточное соблюдение протоколов безопасности, но и с внешними факторами, включая целенаправленные атаки со стороны конкурентов или злоумышленников. Угрозы могут привести к утечке данных, финансовым потерям и снижению доверия клиентов. Исходя из этих вызовов, разработка политики информационной безопасности (ПИБ) должна стать неотъемлемой частью корпоративной стратегии компании.

**Цель:** формирование устойчивой системы защиты данных, которая сможет обеспечивать непрерывность бизнес-процессов и надёжную защиту критически важной информации.

**Задачи:**

1. Определение объектов защиты.
2. Анализ угроз и уязвимостей.
3. Оценка рисков и их влияние на бизнес.
4. Разработка мер защиты и политики безопасности.
5. Внедрение системы управления безопасностью.

**2.2 Объекты защиты**

В логистической отрасли защита информации охватывает широкий спектр элементов, включающих не только клиентские базы и финансовые отчёты, но и данные о маршрутах доставки, складских запасах, а также инфраструктуру мониторинга перемещения грузов. Внедрение GPS-технологий и автоматизированных систем управления повышает удобство контроля, но одновременно делает компанию уязвимой для возможных атак. Несанкционированное проникновение в систему может привести к сбоям в работе, изменению маршрутов или даже к хищению грузов. Помимо технических аспектов, важную роль играет защита персональных данных клиентов и партнёров, поскольку их утечка может нанести серьёзный ущерб репутации компании. Вопрос безопасности также касается внутренней сети организации, серверного оборудования и программного обеспечения, на котором базируется работа логистических процессов. Любое нарушение в этой системе может повлечь за собой значительные финансовые и операционные потери.

Ниже приведены пункты информации, относящиеся к объектам защиты:

1. Клиентские базы данных и персональные данные.
2. Информация о маршрутах и поставках.
3. Логистические системы мониторинга (GPS, трекеры).
4. Системы управления складскими запасами.
5. Финансовые и бухгалтерские данные.
6. Внутренняя сеть и серверное оборудование.
7. Автоматизированные системы учёта и отчетности.

**2.3 Основные угрозы и их источники**

Современные угрозы безопасности в логистической сфере можно разделить на несколько групп в зависимости от их природы.

*Основные угрозы:*

* Кибератаки (вирусные атаки, DDoS, фишинг).
* Несанкционированный доступ и утечка данных.
* Вредоносные действия сотрудников (инсайдерские угрозы).
* Ошибки персонала и недостаточный контроль за доступом.
* Сбои в работе серверов и инфраструктуры.
* Физическое воздействие (кражи оборудования, природные катастрофы).

Некоторые пункты разберём немного подробнее.

Одной из самых распространённых является кибератака, которая может проявляться в виде фишинга, вредоносного программного обеспечения или DDoS-атак, нацеленных на выведение из строя информационных систем. Эти атаки могут иметь разные цели – от кражи данных до нарушения операционной деятельности компании.

Не менее опасными являются угрозы, связанные с действиями самих сотрудников. Даже непреднамеренные ошибки персонала, такие как использование слабых паролей или игнорирование протоколов безопасности, могут привести к утечке информации. Ещё более серьёзными последствиями чреваты инсайдерские угрозы, когда недобросовестные сотрудники намеренно передают данные третьим лицам или злоупотребляют своими привилегиями.

Физическая безопасность также играет важную роль, особенно когда речь идёт о защите серверных помещений и складских объектов. Несанкционированный доступ к этим зонам может привести не только к потере данных, но и к кражам материальных ценностей. Кроме того, следует учитывать возможность природных катастроф и технических сбоев, которые также могут нанести ущерб работе компании.

*Подведём итоги об источниках угроз:*

* Киберпреступники и конкуренты.
* Несанкционированные пользователи.
* Некомпетентность или халатность сотрудников.
* Ошибки в ПО и уязвимости в системах.
* Атаки через третьих лиц (поставщиков, подрядчиков).

**2.4 Оценка угроз, рисков и уязвимостей**

Понимание возможных рисков позволяет более эффективно выстраивать систему защиты. Например, вероятность фишинг-атаки в логистической компании остаётся высокой, поскольку сотрудники часто работают с электронными письмами и документами, содержащими конфиденциальную информацию. Последствия таких атак могут варьироваться от незначительных до критических, в зависимости от уровня подготовки персонала и установленных средств защиты.

Для оценки возможного ущерба логистической компании от реализации потенциальных угроз составляется таблица численной оценки ущерба организации, где каждой качественной степени ущерба соответствует целочисленное значение от 0 до 5. Численные оценки ущерба организации представлены в таблице 2.4.1.

Таблица 2.4.1 – Численная шкала оценки ущерба логистической компании.

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие данных не оказывает влияния на работу логистической компании, моральный и экономический ущерб минимален. |
| 1 | Незначительный ущерб от атаки, который не влияет на выполнение заказов и положение компании на рынке. |
| 2 | Временный сбой в работе логистической системы, задержки поставок, небольшие убытки, но компания сохраняет клиентов и свою позицию на рынке. |
| 3 | Существенные потери данных, нарушение цепочки поставок, потеря доверия клиентов, часть заказчиков переходит к конкурентам. |
| 4 | Критические сбои в логистических процессах, компания на несколько месяцев теряет контроль над поставками, значительные финансовые потери, требуется привлечение крупных инвестиций для восстановления. |
| 5 | Полный крах логистической сети, компания не может выполнять заказы, прекращает деятельность. |

Также необходимо учитывать вероятность того, что реализации каждой потенциальной угрозы вообще будет реализована. Численная классификация вероятностей реализаций различных потенциальных угроз представлена в таблице 2.4.2.

Таблица 2.4.2 – Вероятностно-временная шкала реализации угроз

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид угрозы отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

На основании выше представленных таблиц можно составить таблицу рисков.

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание угрозы** | **Вероятность** | **Потенциальный ущерб** | **Риск** |
| Фишинг-атаки | 0,4 | 3 | 1,2 |
| Вредоносное ПО | 0,2 | 3 | 0,6 |
| Ошибки персонала | 0,3 | 3 | 0,9 |
| Физическое проникновение | 0,1 | 2 | 0,2 |
| Сбои оборудования | 0,3 | 4 | 1,2 |
| **Итог** |  |  | **4,1** |

Сбои в работе оборудования или программного обеспечения также представляют собой серьёзную угрозу, поскольку временная остановка логистических процессов может привести к задержке поставок и значительным убыткам. Важно не только поддерживать оборудование в рабочем состоянии, но и разрабатывать стратегии аварийного восстановления. Это особенно актуально для серверных систем и баз данных, которые должны быть надёжно защищены и регулярно дублироваться.

**2.5 Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов**

* Использование антивирусного ПО и межсетевых экранов.
* Ограничение доступа к критически важным данным.
* Внедрение многофакторной аутентификации.
* Регулярное резервное копирование данных.
* Мониторинг сетевой активности и контроль аномалий.
* Обучение персонала принципам информационной безопасности.
* Разработка регламентов по управлению инцидентами безопасности.

*Разберём немного подробнее.*

Эффективная политика информационной безопасности основывается на комплексном подходе к защите данных. Одним из важнейших инструментов является использование современных антивирусных программ и межсетевых экранов, которые помогают предотвратить проникновение вредоносного кода в корпоративные сети. Однако программная защита должна сочетаться с организационными мерами, такими как контроль за доступом к информации. Ограничение прав пользователей и внедрение многофакторной аутентификации позволяет существенно снизить вероятность утечек.

Важную роль играет обучение персонала. Даже самая совершенная система защиты не будет эффективной, если сотрудники не осведомлены о рисках и не соблюдают базовые правила кибербезопасности. Регулярные тренинги и проверка знаний помогают минимизировать вероятность человеческого фактора в нарушении политики безопасности.

Необходимо также предусмотреть меры по быстрому реагированию на инциденты. В случае обнаружения угрозы важно не только её устранить, но и провести анализ причин, чтобы предотвратить повторные атаки. В этом поможет внедрение систем журналирования событий и оперативного уведомления ответственных лиц.

**Выводы и предложения**

Создание комплексной политики информационной безопасности является критически важным шагом для защиты логистической компании от возможных угроз. Разработанная стратегия позволит минимизировать риски, повысить уровень защищённости данных и обеспечить бесперебойность логистических процессов. Для её успешной реализации необходимо постоянное совершенствование методов защиты, регулярное обновление знаний персонала и адаптация системы безопасности в соответствии с изменяющейся ситуацией.

1. **Ответы на вопросы**
2. **Актуальность и основные причины проблемы информационной безопасности организации, страны**  
   Актуальность проблемы информационной безопасности обусловлена быстрым развитием цифровых технологий, глобальной цифровизацией и ростом количества кибератак. В организациях угроза ИБ возникает из-за недостаточной защиты данных, несоблюдения политик безопасности сотрудниками, а также внешних атак злоумышленников. В масштабах страны риски включают утечки конфиденциальной информации, атаки на критически важные системы (энергетика, транспорт, медицина) и информационную войну. Основными причинами проблем ИБ являются недостаточная осведомленность пользователей, низкая защищённость ИТ-инфраструктуры, нехватка квалифицированных специалистов, а также использование устаревших технологий и отсутствие регулярного мониторинга угроз.
3. **Цели и задачи политики информационной безопасности**  
   Целью политики информационной безопасности является обеспечение конфиденциальности, целостности и доступности информации. Основные задачи включают разработку и внедрение правил и процедур защиты данных, контроль доступа, мониторинг угроз, реагирование на инциденты, обучение сотрудников основам ИБ и обеспечение соответствия законодательным требованиям.
4. **Основные угрозы информационной безопасности организаций**  
   Каждая организация сталкивается с уникальными угрозами, зависящими от её специфики. Например, в учебных заведениях критичны утечки данных студентов и преподавателей, в банках – хищение финансовых средств, а в логистических компаниях – нарушение маршрутов доставки и кража грузов. Основные угрозы включают несанкционированный доступ, вредоносное ПО, фишинговые атаки, утечки данных, ошибки сотрудников, физическое воздействие (кражи оборудования) и внутренние угрозы со стороны персонала.
5. **Оценка рисков в информационной безопасности**  
   Оценка рисков включает несколько этапов:

* **Идентификация активов**: определение ценных данных и систем.
* **Анализ угроз**: выявление возможных атак и уязвимостей.
* **Оценка вероятности угроз**: определение вероятности возникновения инцидента.
* **Анализ последствий**: определение потенциального ущерба.
* **Расчёт рисков**: комбинация вероятности и ущерба для приоритезации защиты.
* **Выбор мер снижения рисков**: внедрение технических и организационных мер защиты.

1. **Программа внедрения политики информационной безопасности**  
   Программа внедрения должна включать следующие элементы:

* Разработка нормативных документов, регламентов и инструкций.
* Организация обучения сотрудников.
* Внедрение технических средств защиты (антивирусное ПО, системы мониторинга, межсетевые экраны).
* Регулярные аудиты и тестирования на проникновение.
* План реагирования на инциденты и резервное копирование данных.
* Постоянное обновление политики безопасности с учётом новых угроз.

