|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА  Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)** |
| **Кафедра КБ-3 «Управление и моделирование систем»** |

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ** | |
| **по дисциплине** | |
| **«Основы информационной безопасности»** | |
|  | |
| Выполнил студент группы БИСО-01-19 19Б0101 | **Устинова Алина Александровна** |
| Принял Ассистент - Кафедры КБ-2 «Прикладные информационные технологии» - Институт комплексной безопасности и специального приборостроения | **Изергин Д.А.** |

|  |  |  |
| --- | --- | --- |
| Практическая работа выполнены | «\_\_»\_\_\_\_\_\_\_202\_\_ г. |  |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_202\_\_ г. |  |

Москва 2020

**Практическая работа №1**

**«Политика безопасности»**

**Задание:**

1.Составить политику информационной безопасности для собственной

организации.

2.Составить технический регламент, инструкцию для одного из

отделов.

**Ход работы:**

**1.** Составить политику информационной безопасности для собственной

организации.

Компания ООО «МастерКом»

Штаб – 45 сотрудников.

• член совета директоров(1);

• представитель руководства компании (СЕО, финансовый директор, директор по развитию) (1);

• СЮ (директор службы автоматизации) (1);

• CISO (директор по информационной безопасности) (1);

• аналитик службы безопасности (5);

• аналитик ИТ-службы (5);

• представитель юридического отдела (1);

• представитель от пользователей (5);

• технический писатель (5);

• менеджеры по работе с клиентами (20);

• отдел информационной безопасности (5).

Аналитик службы безопасности выполняет анализ различных угроз и ищущий способы защиты от них, предотвращает утечку информации и занимается разработкой программного обеспечения в сфере информационной безопасности.

Аналитик ИТ-службы решает сложные организационно-технические проблемы, имеющие междисциплинарную природу, использующие принципы общей теории систем и методы системного анализа.

Задачи представителя юридического отдела являются: Обеспечение соблюдения предписаний законодательных актов на предприятии и защита его интересов. В рамках этого направления осуществляется поиск, обобщение и анализ нормативных актов, необходимых для работы фирмы; Организацию и ведение систематизированного учета, хранение правовых документов, поступающих на предприятие; Приобретение и использование электронных баз нормативной информации; Учет локальных документов, утверждаемых на предприятии; Подписка на официальные издания, в том числе электронные, в которых публикуются правовые акты по трудовой, налоговой, хозяйственной, финансовой и прочей деятельности; Проверка соответствия требованиям законодательства проектов приказов, положений, инструкций и прочих документов, предоставляемых на подпись директору. В рамках этого направления определяется правомочность руководителя издавать соответствующий акт, степень необходимости согласования его с подразделениями фирмы, правильность ссылок на нормы; Визирование проектов, которые составлены в соответствии с установленными требованиями; Проверку этапов согласования с подразделениями фирмы; Возврат проектов документов без визы в отделы, их разработавшие. При этом составляется письменное заключение, где указываются положения, противоречащие нормам, приводятся ссылки на правовые документы, инструкции и пр.; Контроль приведения проектов в соответствие с нормативной базой; Выдача руководителям подразделений предписаний для изменения либо отмены актов, которые были изданы с нарушениями.

Технические писатели отвечают за написание всех сопутствующих IT-продукту текстов: от интерфейсных подсказок пользователям до технической документации, которой пользуются разработчики.

Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет.

**2.** Составить технический регламент, инструкцию для одного из

отделов.

Отдел информационной безопасности

1. Общие положения

1.1. Регламент информационной безопасности Департамента административных органов и общественной безопасности администрации Владимирской области (далее – Департамент) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Департамент в своей деятельности.

1.2. Настоящий Регламент распространяется на всех сотрудников Департамента, подведомственных учреждений, сотрудников аппарата мировых судей Владимирской области  и обязателен для исполнения всеми сотрудниками и должностными лицами. Положения настоящего Регламента применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.3. Период действия и порядок внесения изменений

Настоящий Регламент вводится в действие приказом директора Департамента.

Регламент признается утратившим силу на основании приказа директора Департамента.

Изменения в Регламент вносятся приказом директора Департамента.

Инициаторами внесения изменений в Регламент информационной безопасности являются:

-          Директор Департамента;

-          Заместитель директора

-          Администратор информационной безопасности;

2. Термины, определения, сокращения

2.1. Термины и определения

*Автоматизированная система* – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

*Администратор информационной безопасности* – специалист Департамента, осуществляющий контроль за обеспечением защиты информации в ЛВС, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

*Аудит информационной безопасности* – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как  Департаментом  (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

*Аутентификация* – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

*Доступ к информации* – возможность получения информации и ее использования.

*Защищенный канал передачи данных* – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

*Идентификация* – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

*Информация* – это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

*Информационная безопасность* – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

*Информационная система* – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач отделов Департамента. В Департаменте используются различные типы информационных систем для решения управленческих, учетных, обучающих и других задач.

*Источник угрозы* – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

*Конфиденциальная информация* – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

*Конфиденциальность* – доступ к информации только авторизованных пользователей.

*Критичная информация* – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование отделов Департамента, привести к причинению в Департаменте материального или иного вида ущерба.

*Локальная вычислительная сеть (ЛВС)* – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

*Межсетевой экран (МЭ)* – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью Департамента и внешними сетями (сетью Интернет).

*Несанкционированный доступ к информации (НСД)* – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

*Регламент информационной безопасности* – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

*Пользователь ЛВС* – сотрудник Департамента (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

*Программное обеспечение* – совокупность прикладных программ, установленных на сервере или ЭВМ.

*Регистрационная (учетная) запись пользователя* – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название отдела, телефоны, E-mail и т.п.

*Системный администратор* – сотрудник Департамента, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

*Средства криптографической защиты информации* – средства шифрования, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

*Угрозы информационным данным* – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

*Управление информационной безопасностью* – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

*Уязвимость* – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

*Целостность информации* – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

*ЭВМ* – электронная - вычислительная машина, персональный компьютер.

*Электронная цифровая подпись* – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

*VPN (VIRTUAL PRIVATE NETWORK)* – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

2.2. Сокращения

АС – Автоматизированная система.

БД – База данных.

ЗИ – Защита информации.

ИБ – Информационная безопасность.

ИС – Информационная система.

ИТС – Информационно-телекоммуникационная система.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПО – Программное обеспечение.

СВТ – Средства вычислительной техники.

СЗИ – Средство защиты информации.

СКЗИ – Средство криптографической защиты информации.

СПД – Система передачи данных.

СУБД – Система управления базами данных.

СУИБ – Система управления информационной безопасностью.

СЭД – Система электронного документооборота.

ЭВМ – Электронная - вычислительная машина, персональный компьютер.

ЭЦП – Электронная цифровая подпись.

3. Описание процесса

3.1. Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства с целью выявления уязвимостей информационных активов.

- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ, корректировка моделей угроз и нарушителя.

- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию.

- Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

4. Ответственность

4.1. Ответственность за нарушение  информационной безопасности несет каждый сотрудник Департамента в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования Регламента, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Департаменту в результате нарушения ими Регламента  (Ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Департамента несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

5. Контроль

5.1. Контроль за исполнением требований настоящего Регламента и поддержанием ее в актуальном состоянии возлагается на администратора информационной безопасности.

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

Ответственность за реализацию Регламента возлагается: в части, касающейся исполнения правил регламента, – на каждого сотрудника Департамента, согласно должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящего Регламента.