МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

ФАКУЛЬТЕТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

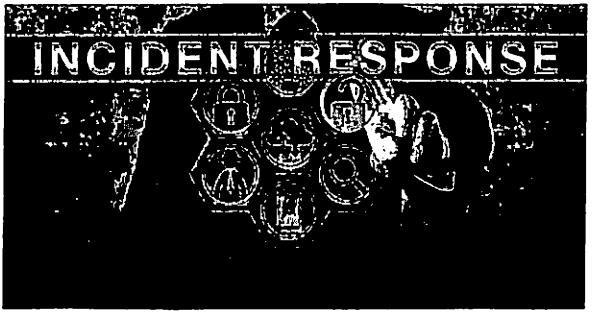
Кафедра обеспечения информационной безопасности

А.А. Абдурахманов
З.И. Азизова

МЕТОДИЧЕСКОЕ ПОСОБИЕ

к лабораторным работам по предмету

«Инциденты атак и реагирование на них»



Ташкент 2021

Составители: А.А. Абдурахманов, З.И. Азизова, «Инциденты атак и реагирование на них». ТУИТ имени Мухаммада ал-Хоразмий. Ташкент, 2021. 68 стр.

Настоящие методические указания предназначены для оказания методической помощи студентам 4-го курса при выполнении лабораторных работ по курсу «Инциденты атак и реагирование на них».

Методическое пособие содержит 10 лабораторных работ, в которых изложены сведения о принципах и основных действиях по управлению процессом менеджмента инцидентов информационной безопасности, в нем также изложены принципы и подходы к обеспечению безопасности персонала, физической безопасности, исследованию контроля доступа и т.д. позволяющие ознакомиться со всем многообразием процедур и мероприятий необходимых для проведения оперативного реагирования на инциденты информационной безопасности.

Каждая лабораторная работа сопровождается заданиями и вопросами для самопроверки, что способствует закреплению материала.

Рекомендовано к печати решением учебно-методического совета ТУИТ имени Мухаммада ал-Хоразмий (протокол №9(134) "27" "04" 2021г.)

Формат 60×80 1/16. Печ.лист 4,25.
Заказ № 32 Тираж 10.
Отпечатано в «Редакционно издательском»
отделе при ТУИТ.
Ташкент ул. Амир Темур, 108.

Лабораторная работа № 1

Тема: Анализ основных направлений политики обеспечения ИБ

Цель работы: приобретение навыков построения политики ИБ с учетом правовых, морально-этических, технологических, организационных, физических мер защиты.

1. Теоретические сведения:

Событие ИБ — идентифицированное появление определённого состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности. *Инцидент ИБ* — появление одного или нескольких нежелательных, или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ для функционирующей информационной системы, компьютерной системы или организации в целом.

По способам осуществления все *меры защиты информации*, ее носителей и систем ее обработки подразделяются на правовые (законодательные), морально-этические, технологические, организационные (административные и процедурные), физические, технические (аппаратурные и программные).

К *правовым мерам защиты* относятся действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы

К *морально-этическим мерам* защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как требования нормативных актов, однако, их несоблюдение ведет обычно к падению авторитета или престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т.п.) правил или предписаний.

К *технологическим* относятся разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии разрешений от нескольких должностных лиц, процедур проверки соответствия реквизитов, исходящих и входящих сообщении в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т.п.

Организационные меры защиты - это меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических

препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов АС (пломбы, наклейки и т. п.).

Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

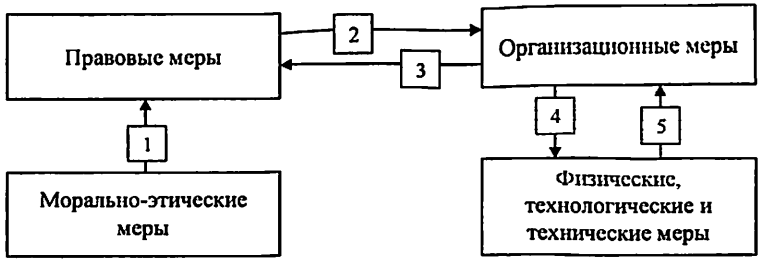


Рисунок 1. Взаимосвязь мер обеспечения информационной безопасности

1. Нормативные и организационно-распорядительные документы составляются с учетом и на основе существующих норм морали и этики;
2. Организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации;
3. Воплощение организационных мер требует разработки соответствующих нормативных и организационно-распорядительных документов;
4. Для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами;
5. Применение и использование технических средств защиты требует соответствующей организационной поддержки.

В рамках внутренней обработки инциденты в зависимости от затронутых ресурсов можно классифицировать следующим образом:

Степень критичности инцидента	Характеристика
Высокая критичность	Инциденты, связанные с ключевыми ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию)
Средняя критичность	Инциденты, связанные с некритичными ресурсами серверного сегмента
Низкая критичность	Инциденты, связанные с некритичными ресурсами пользовательского сегмента (рядовой пользователь)

Отчеты о событиях и инцидентах информационной безопасности. Форма отчета о событиях и инцидентах ИБ предназначена для обеспечения информации о событии ИБ, а затем, в случае если оно определено как инцидент ИБ, то и об инциденте ИБ, для определенных лиц.

Если подозревается, что событие ИБ развивается или уже свершилось, особенно событие, которое может привести к существенным потерям или ущербу собственности, или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная информация будет использована для инициирования соответствующего процесса оценки, которая определит, должно ли это событие категорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения (ограничения потерь) или ущерба, следует предпринять. Поскольку процесс оценки по своему характеру является краткосрочным, то в данный момент необязательно заполнять все поля формы отчета.

Если сотрудник является членом группы обеспечения эксплуатации системы, анализирующим полностью/частично заполненные формы отчета, то он должен принять решение, надо ли отнести данное событие к категории инцидента. ИБ. При положительном решении сотрудник должен внести в

форму отчета об инциденте ИБ как можно больше информации и передать формы отчетов о событии и инциденте ИБ в группу реагирования на инциденты ИБ (ГРИИБ). *Независимо от того, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена.*

Если сотрудник является сотрудником ГРИИБ, анализирующим формы отчетов о событиях и инцидентах ИБ, переданные членом группы обеспечения эксплуатации, то форма отчета об инциденте ИБ должна обновляться по ходу расследования и, соответственно, должна обновляться база данных событий/инцидентов ИБ.

При заполнении форм следует соблюдать следующие *рекомендации*:

- *по возможности формы отчета должны заполняться и передаваться в электронном виде.* В случае, если существуют проблемы или считается, что существуют проблемы с принятыми по умолчанию механизмами электронного оповещения (например, электронная почта), включая случаи, когда система может подвергаться атаке и формы отчета могут быть прочитаны несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть телефон или текстовые сообщения, а также использование курьеров
- *следует представить информацию, основанную на фактах*, в которой сотрудник уверен, не следует что-либо придумывать для того, чтобы заполнить все формы. Если сотрудник считает уместным включить иную информацию, которую не может подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее недостоверности;
- *следует подробно указать, как можно связаться с сотрудником.* Немедленно или спустя некоторое время может возникнуть необходимость контакта с ним для получения дальнейшей информации, касающейся Вашего отчета.

Если позднее сотрудник обнаружит, что какая-либо представленная им информация неточна, неполна или ошибочна, то следует внести поправки в отчет и представить его повторно.

2. Задание к лабораторной работе:

Заполните форму отчета о событии информационной безопасности либо об инциденте информационной безопасности, основываясь на форму отчета, приведенную в стандарте O'z DSt ISO/IEC 27035:2015 (Приложение D.2 (D.2.1., D.2.2., D.2.3.), D.4)

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Что Вы понимаете под системой? Приведите примеры систем. Перечислите элементы приведенной Вами системы.*
2) *Дайте определение понятия «информационная система».*
3) *В чем различие понятий информационная система и информационная технология?*
4) *Дайте определение понятия «аудит»?*
5) *В чем заключается назначение аудита информационной безопасности?*
6) *Назовите составляющие услуги аудита?*
7) *Перечислите цели проведения аудита безопасности?*
8) *Для чего необходим контроль состояния защиты информации?*

Лабораторная работа № 2

Тема: Разработка положений, регламентов и процессов взаимодействия для решения организационных задач безопасности

Цель работы: практическое освоение и приобретение навыков формирования организационных мер по обеспечению безопасности предприятия.

1. Теоретические сведения:

Мероприятия по защите информации организационного характера не ограничиваются разработкой положений. Для этого также необходимо произвести:

- документирование и оптимизацию бизнес-процессов;
- установку градации сотрудников и их уровней доступа к информации, содержащей коммерческую тайну;
- создание подразделений или назначение лиц, ответственных за обеспечение информационной безопасности, иногда изменение структуры предприятия в соответствии с требованиями безопасности;
- информирование или переобучение персонала;
- организацию мероприятий по тестированию подготовки персонала к работе с системой в критических ситуациях;
- получение лицензий, например, на работу с государственной тайной;
- обеспечение технической защиты помещений и оборудования с дальнейшей сертификацией классов защиты, определение их соответствия нормативно-правовым требованиям;
- создание системы безопасности для цепочки поставщиков, во взаимодействии с которыми передаются конфиденциальные данные, внесение в договоры с контрагентами оговорок о сохранении коммерческой тайны и мер ответственности за ее разглашение;
- установка пропускной системы для сотрудников, выдача им электронных средств идентификации;

- выполнение всех требований законодательства по защите персональных данных;
- разработка системы взаимодействия с государственными органами в случае запроса ими у организации информации, которая может быть отнесена к конфиденциальной.

Форум по координации вопросов, связанных с внедрением средств обеспечения ИБ.

- выработка соглашений о разграничении ответственности за обеспечение информационной безопасности внутри организации;
- выработка специальных методик и политик, связанных с информационной безопасностью: анализ рисков, классификация систем и информации по уровням безопасности;
- поддержание в организации «атмосферы» информационной безопасности, в частности, регулярное информирование персонала по этим вопросам;
- обеспечение обязательности учета вопросов информационной безопасности при стратегическом и оперативном планировании;
- обеспечение обратной связи (оценка адекватности принимаемых мер безопасности в существующих системах) и координация внедрения средств обеспечения информационной безопасности в новые системы или сервисы;
- анализ инцидентов в области информационной безопасности, выработка рекомендаций;

Распределение ответственности за обеспечение безопасности:

1. Определение ресурсов, имеющих отношение к информационной безопасности, по каждой системе;
2. Для каждого ресурса (или процесса) должен быть назначен ответственный сотрудник из числа руководителей. Разграничение ответственности должно быть закреплено документально;
3. Для каждого ресурса должен быть определен и закреплен документально список прав доступа (матрица доступа)

Процесс внедрения новой информационной системы:

1. Новая система должна соответствовать существующей политике управления пользователями, где указываются цели и задачи пользователей, а также в обязательном порядке согласовываться с руководителем, ответственным за обеспечение безопасности данной системы;
2. Все внедряемые компоненты должны быть проверены на совместимость с существующими частями системы.

2. Задание к лабораторной работе:

Проанализируйте приведенную ниже ситуацию. Что организации необходимо предпринять в первую очередь, для того чтобы уменьшить возможный ущерб? Заполните и предоставьте доклад о расследовании, включая данные и результаты криминалистического расследования.

Ситуация: *Пользователи не могут войти в домен, корпоративная сеть неработоспособна....*

Клиент: Крупная международная юридическая фирма

Инцидент: В 2 часа ночи корпоративная сеть перестала работать:

1. Пользователи не могли войти в сеть или в домен Windows;
2. Вся корпоративная сеть была неработоспособна;
3. Все почтовые службы отключились.

Дополнительная информация: Клиент - крупная юридическая фирма, имеющая заметный общественный резонанс. Первоначально предполагалось, что это будет целенаправленная атака. В многочисленных средствах массовой информации были написаны отчеты о сложных возможностях взлома, которые предоставляет конкретная группа.

Действия, предпринятые в ходе криминалистического анализа:

- группа по реагированию на инциденты и судебно-криминалистическому анализу была направлена на сайт клиента в течение 4 часов;
- все доступные улики были визуализированы и занесены в резервную копию;
- журналы были собраны с внутренних/внешних веб серверов, брандмауэра, маршрутизаторов, IDS/IPS, журналов событий Windows;

- файлы улик, полученные с жестких дисков сервера, были проанализированы;
- все собранные журналы были соотнесены и проанализированы;
- были проанализированы службы и процессы на затронутых компьютерах;
- были проанализированы конфигурации серверов, маршрутизаторов и брандмауэров Windows;
- каждый шаг исследования был подробно документирован.

Результаты:

1. Группа реагирования обнаружила сложную бот-сеть с установленным командным и управляющим программным обеспечением.
2. Бот-сеть изменила политики безопасности на серверах, не позволяя авторизованным пользователям входить в систему.
3. Бот-сеть представляла собой совершенно новую форму вредоносного ПО, и до 5 дней не было доступно никакой публичной информации.
4. Коренная причина уязвимости была определена ГРИИБ из-за неправильной настройки брандмауэра.
5. ГРИИБ предоставила отчет об анализе и рекомендации по устранению первопричины.
6. ГРИИБ помогла клиенту с устранением первопричины и восстановила работу сети и электронной почты.
7. По результатам анализа команда ГРИИБ пришла к выводу, что данный случай не является результатом целенаправленной атаки.

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1. *В чем состоит важность и необходимость процесса принятия новой информационной системы?*
2. *Как распределять ответственность за обеспечение безопасности внутри организационной структуры?*
3. *Каким образом осуществляется оценка адекватности принимаемых мер безопасности в имеющихся системах?*
4. *Для чего необходима выработка специальных методик и политик, таких как анализ рисков, классификация систем и информации по уровням безопасности?*
5. *Зачем нужно создавать форумы по ИБ?*
6. *Каким образом форумы ИБ связаны с этапом извлечения уроков процесса менеджмента инцидентов ИБ?*

Лабораторная работа № 3

Тема: Анализ видов ресурсов и управление ресурсами по ограничению инцидентов ИБ

Цель работы: выработка у студентов навыков управления ресурсами и непрерывностью бизнеса.

1. Теоретические сведения:

Инвентаризация ресурсов помогает обеспечить эффективность мер безопасности и может способствовать достижению других целей, например, обеспечению здоровья и личной безопасности, страхованию и управлению активами. Инвентаризация должна проводиться в отношении основных ресурсов каждой информационной системы. Каждый компонент ресурсов должен быть четко определен в соответствии с классификацией по его принадлежности и применяемым к нему мерам безопасности. Примерами ресурсов, ассоциирующихся с информационными системами, могут быть:

1. *Информационные ресурсы:* базы данных и файлы данных, системная документация, пользовательская документация, учебные материалы, инструкции по эксплуатации или по поддержке, планы по поддержанию непрерывности бизнеса, мероприятия по устранению неисправностей, архивы информации или данных;
2. *Программные ресурсы:* приложения, операционные системы и системное программное обеспечение, средства разработки приложений и утилиты;
3. *Физические ресурсы:* вычислительная техника (процессоры, мониторы, переносные компьютеры), коммуникационное оборудование (маршрутизаторы, телефонные станции, факсы, автоответчики, модемы), магнитные носители (кассеты и диски), другое техническое оборудование (источники питания, кондиционеры), мебель, помещения;
4. *Вычислительные и коммуникационные сервисы, вспомогательные услуги:* отопление, освещении, энергоснабжение, кондиционирование воздуха и т.п.

Классификация ресурсов. Классификация ресурсов должна использоваться для определения необходимости принятия мер безопасности, их объема и приоритетности. Ресурсы имеет различную степень уязвимости и важности. Отдельные компоненты могут нуждаться в дополнительной защите или в особом обращении. Для определения соответствующих уровней обеспечения безопасности и информирования пользователей о необходимости особого обращения с информацией и ресурсами должна использоваться система классификации мер безопасности.

Принципы классификации:

При классификации мер безопасности и определении соответствующих мероприятий по защите информации следует принимать во внимание необходимость предоставления информации, а также последствия несанкционированного доступа или разрушения информации. В частности, следует обратить внимание на следующие факторы:

- *конфиденциальность:* производственная необходимость предоставления или ограничения доступа к информации с соблюдением конфиденциальности и контроля, требуемых в отношении ограниченного доступа к информации;
- *целостность:* производственная необходимость проверки изменений информации и контроль, необходимый для защиты правильности и полноты информации
- *доступность:* производственная необходимость иметь доступ к информации и соблюдение принятых видов контроля для ее получения.

Ответственность за определение классификационной принадлежности единицы информации, например, документа, записи данных, файла данных или дискеты, а также за периодичный пересмотр классификации должна лежать на лице, подготовившем данные, или на владельце данных.

Следует уделить особое внимание интерпретации классификационных меток на документах, поступающих от других организаций, которые могут быть различными в отношении одной и той же информации либо похожими.

Все ресурсы должны быть классифицированы по степени важности. *Для каждого класса должны быть регламентированы следующие действия:*

- копирование;
- хранение;
- передача почтой, факсом, электронной почтой;
- передача голосом, включая мобильные телефоны, голосовую почту уничтожение.

2. Задание к лабораторной работе:

Проанализируйте приведенную ниже ситуацию. Что организации необходимо предпринять для

Ситуация: *Свидетельства взлома были обнаружены на веб-сервере с HIPAA (акт США о передаче и защите данных учреждений здравоохранения).*

Клиент: Крупная медицинская компания

Инцидент: После того, как фирма, занимавшаяся разработкой оригинальных веб-приложений, отправилась на новый проект, вновь нанятая фирма обнаружила следы улик от хакерских групп:

1. Веб-сервер был взломан.
2. База данных и веб-сервер находились на одном и том же физическом сервере, и к работе были привлечены данные, регулируемые HIPAA.
3. Инцидент произошел за 4 месяца и в течение 5 дней, основываясь на первоначальных выводах новой фирмы-разработчика.
4. В течение этих 5 дней не было доступно никаких логов, кроме логов веб-сервера.
5. Клиент должен был знать размер ущерба, а также должен ли он принимать правовые меры, такие как предоставление уведомления о нарушении (-ях) и сообщение о нарушении (-ях) Генеральному прокурору.

Действия, предпринятые во время проведения криминалистического анализа:

- были собраны веб-серверные технологии, платформа разработки и язык программирования;
- предоставлена информация о сервере базы данных и резервная копия базы данных;
- были собраны ограниченные лог-файлы веб-сервера;
- ГРИИБ исследовала атаки на веб-приложение;
- ГРИИБ создала среду криминалистического анализа для анализа веб-приложения и базы данных;
- ГРИИБ проанализировала базу данных, чтобы определить происхождение и масштаб атаки;
- ГРИИБ коррелировала логи веб-сервера с данными о деятельности базы данных;
- каждый шаг исследования был подробно документирован.

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Какую категорию ресурсов включает в себя Инвентаризация ресурсов?*
2) *Приведите в отчете к практической работе классификацию ресурсов.*
3) *На какие факторы слудует обращать внимание при классификации мер безопасности и определении соответствующих мероприятий по защите информации?*
4) *Приведите пример инвентаризации ресурсов организации по разработке программных средств защиты информации.*

Лабораторная работа № 4

Тема: Составление программы обеспечения безопасности персонала

Цель работы: приобретение навыков составления программы проверки действий персонала при нештатных ситуациях.

1. Теоретические сведения:

Безопасность при выборе и работе с персоналом:

1. Необходимо включить задачу обеспечения безопасности в служебные обязанности всех сотрудников.
2. Проверка персонала при приеме на работу:
   - проверка рекомендаций;
   - проверка данных из резюме;
   - подтверждение ученых степеней и образования;
   - идентификация личности.
3. Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками.
4. Условия трудового соглашения с работником.

Реакция на инциденты ИБ и неисправности:

1. Отчеты об инцидентах.
2. Отчеты о недостатках в системе безопасности.
3. Отчеты о сбоях и неисправностях компьютерных систем.
4. В случае обнаружения нестандартной ситуации необходимо:

- записать все симптомы ее появления;
- компьютер должен быть изолирован и если возможно его использование приостановлено;
- о факте должно быть немедленно сообщено непосредственному руководителю и службе информационной безопасности, они же должны быть проинформированы о результатах анализа причин произошедшего;
- запрещается предпринимать самостоятельные меры без разрешения уполномоченных лиц;

5. Дисциплинарные меры (в зависимости от последствий: дисциплинарные, административные или даже уголовные).
6. Регулярное обучение персонала по вопросам безопасности.

2. Задание к лабораторной работе:

1. Сформулируйте краткую программу проверки персонала при приеме на работу. Основываясь на первоначальные по вашему мнению критерии.
2. Изучите следующий сценарий и определите вопросы, связанные с решением возникшего инцидента.

Сценарий: Отказ в обслуживании сервера системы доменных имен (DNS) в субботу днем у внешних пользователей начинают возникать проблемы с доступом к публичным веб-сайтам организации. В течение следующего часа проблема усугубляется до такой степени, что практически каждая попытка получить доступ к любому из публичных веб-сайтов организации терпит неудачу. Между тем, сотрудник сетевой службы организации отвечает на автоматически генерируемые предупреждения с пограничного маршрутизатора и определяет, что большая часть пропускной способности интернет-портала организации потребляется необычайно большим количеством пакетов User Datagram Protocol (UDP) от обоих серверов публичной системы доменных имен (DNS) организации. Анализ трафика показывает, что DNS-серверы получают большие объемы запросов с одного внешнего IP адреса. Сетевой администратор также замечает, что все DNS-запросы с этого адреса имеют порт источника либо UDP 7, либо UDP 19. Во время проведения этого анализа датчики обнаружения вторжения в сеть организации записывают подозрительную активность, связанную со службами эхо и чарген.

Дополнительные вопросы сценария:

1. С кем следует связаться организации относительно внешнего IP-адреса, используемого во всех пакетах?

2. Предположим, что после того, как были приняты первоначальные меры по сдерживанию, сетевые администраторы обнаружили, что девять

внутренних хостов также пытались выполнить те же самые необычные запросы к DNS-серверу. Как это повлияет на обработку этого инцидента?

3. Предположим, что два из девяти внутренних узлов покинули сеть до того, как с их системными администраторами связались. Как будут идентифицированы владельцы системы?

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1. *Что Вы понимаете под безопасностью при выборе персонала?*
2. *Зачем нужна проверка персонала при приеме на работу?*
3. *Нужно ли реагировать на секьюрити инциденты и неисправности? Обоснуйте ответ.*
4. *С какой целью составляется соглашение о соблюдении режима информационной безопасности со всеми сотрудниками*

Лабораторная работа № 5

Тема: Исследование методики обеспечения физической безопасности в организации

Цель работы: совершенствование навыков формирования правил программы реагирования на инциденты ИБ с учетом физических составляющих организации.

1. Теоретическая часть:

Безопасность оборудования:

1. Оборудование должно располагаться с учетом требования минимизации доступа в рабочее помещение лиц, не связанных с обслуживанием этого оборудования.
2. Системы обработки и хранения информации, содержащие важные данные, должны быть расположены так, чтобы минимизировать возможность случайного или преднамеренного доступа к ним неуполномоченных лиц в процессе их обработки.
3. Объекты, требующие специальной защиты, должны быть изолированы.
4. Меры защиты должны быть приняты для минимизации следующих потенциальных угроз: кража, огонь, взрыв, дым, вода, пыль, вибрация, химические вещества, побочные электромагнитные излучения и наводки.
5. Политика компании должна запрещать прием пищи, напитков и курение вблизи оборудования.
6. Оборудование должно подвергаться регулярным осмотрам и дистанционному контролю с целью обнаружения признаков, которые могут повлечь за собой отказ системы.
7. Использование специальных средств защиты, таких как накладка на клавиатуру, необходимых в случае расположения оборудования в промышленных зонах.

8. Должны быть учтены воздействия от происшествий на соседних объектах (пожар у соседей, наводнение или затопление верхнего этажа, взрыв на улице и т.д.)

Безопасность кабельной системы:

1. Силовые и телекоммуникационные линии в информационно-обрабатывающую систему должны проходить под землей (если возможно). В противном случае, им требуется адекватная альтернативная защита.
2. Сетевые кабели должны быть защищены от несанкционированного подключения или повреждения. Этого можно достигнуть при помощи их прокладки вне общедоступных зон.
3. С целью снижения влияния электромагнитных помех, силовые кабели должны быть разделены с коммуникационными.
4. Для важных или особо важных систем должно быть предусмотрены следующие меры защиты:
   - линии связи должны быть закрыты защитными коробами, кроссовые помещения и шкафы должны надежно запираться и опечатываться; контроль целостности должен осуществляться регулярно;
   - линии связи должны быть продублированы;
   - применение оптического кабеля;
   - обнаружение несанкционированных подключений к линиям связи и оповещение персонала.

Безопасное уничтожение отработавшего оборудования:

1. Устройства хранения информации, содержащие ценную информацию, при выведении из эксплуатации должны быть физически уничтожены, либо должно быть проведено гарантированное стирание с них остаточной информации.
2. Все оборудование, включая носители информации, перед передачей его другому владельцу (или списанием) должно быть проверено на предмет отсутствия в нем важной информации или лицензионного программного обеспечения.

3. Дальнейшая судьба поврежденных устройств хранения, содержащих важную информацию, (уничтожение или ремонт) определяется на основе заключения экспертной комиссии.

Безопасность рабочего места:

- документы на всех видах носителей и вычислительная техника, в случае если ими не пользуются, а также в нерабочее время, должны храниться в запираемом помещении.
- ценная информация, когда она не используется, должна храниться в защищенном месте (огнеупорный сейф, выделенное помещение).
- персональные компьютеры, терминалы и принтеры не должны оставаться без присмотра во время обработки информации и должны защищаться блокираторами клавиатуры, паролями или иными методами на время отсутствия пользователя.
- должны быть приняты надежные меры, исключающие несанкционированное использование копировальной техники в нерабочее время.
- распечатки, содержащие ценную (конфиденциальную) информацию должны изыматься из печатающего устройства немедленно.

2. Задание к лабораторной работе:

1. Разработайте правила по обеспечению физической безопасности с учетом деятельности организации (выбор организации по желанию) и опишите способы распространения и донесения данных правил до всех сотрудников организации.
2. Проанализируйте приведенный сценарий.

Сценарий 5: *Скомпрометированный сервер баз данных*

Во вторник вечером администратор базы данных выполняет некоторые нерабочие часы обслуживания на нескольких производственных серверах баз данных. Администратор замечает некоторые незнакомые и необычные имена каталогов на одном из серверов. Просмотрев список каталогов и некоторые

файлы, администратор приходит к выводу, что сервер подвергся атаке, и вызывает на помощь группу реагирования на инциденты. В результате расследования команды выясняется, что 6 недель назад злоумышленник успешно получил root доступ к серверу.

Дополнительные вопросы для этого сценария:

1. Из каких источников команда могла бы определить, когда произошел компромисс?
2. Как бы изменилась обработка этого инцидента, если бы команда обнаружила, что на сервере баз данных был запущен анализатор пакетов и перехват паролей из сети?
3. Как бы изменилась обработка этого инцидента, если бы команда обнаружила, что на сервере выполнялся процесс, который копировал бы базу данных, содержащую конфиденциальную информацию о клиенте (включая личную информацию) каждую ночь и отправлял бы ее по электронной почте на внешний адрес? 4. Как бы изменилась обработка этого инцидента, если бы команда обнаружила руткит, установленный на сервере?

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Что включает в себя безопасность оборудования?*
2) *Почему необходимо предусматривать безопасность кабельной системы?*

3) *Какие мероприятия предусмотрены безопасным уничтожением оборудования при его списывании?*

4) *Что подразумевается под обеспечением безопасности рабочего места?*

Лабораторная работа № 6

Тема: Организация менеджмента коммуникациями и процессами

Цель работы: приобретение навыков и умений грамотного составления служебных инструкций по реагированию на инциденты ИБ и их предотвращению.

1. Теоретические сведения:

Служебные инструкции и ответственность. Должностные инструкции должны включать:

- порядок обработки и обращения с информацией;
- порядок взаимодействия с другими системами, разрешенные часы доступа на рабочее место (в ночное время, в выходные);
- порядок действий в нештатных ситуациях;
- список лиц и способы связи с ними в нештатных ситуациях;
- специальные инструкции по обращению с результатами обработки информации, в том числе конфиденциальными и ошибочно обработанными;
- рестарт системы и восстановительные процедуры, необходимые в случае сбоя системы.

Контроль изменений в операционной среде:

1. Идентификация и запись важных изменений.
2. Оценка потенциального последствий таких изменений.
3. Формальное утверждение процедуры внесения изменений.
4. Взаимодействие со всеми заинтересованными лицами при внесении изменений.
5. Процедуры определения ответственности и возврата в исходное состояние при неудачных попытках изменений.

Процедуры реагирования в случае инцидентов. Процедуры должны предусматривать все возможные ситуации, включая:

- сбои в информационных системах;

- отказ в обслуживании;
- ошибки из-за неполных или неправильных входных данных;
- утечку информации;

В дополнении к оперативному плану восстановления процедуры должны также включать:

- анализ и определение причин инцидента;
- планирование и внедрение мер для предотвращения повторения (если необходимо);
- анализ и сохранение сведений об инциденте, которые можно представить в качестве доказательства (улики, свидетельства и т.п.);
- определение порядка взаимодействия между пострадавшими от инцидента и участниками процесса восстановления;
- обязательное информирование ответственных лиц.

Служебные инструкции и ответственность. *Процедуры реагирования в случае инцидентов:* по каждому инциденту должно быть собрано максимальное количество информации, которой также необходимо обеспечить необходимый уровень защиты для:

- последующего анализа внутренних проблем;
- использования собранных данных для привлечения виновных к дисциплинарной, административной или уголовной ответственности;
- использования при ведении переговоров о компенсациях с поставщиками аппаратного и программного обеспечения.

Действия по восстановлению после обнаружения уязвимостей в системе безопасности, исправлению ошибок и ликвидации неисправностей должны быть внимательно и формально запротоколированы. Процедура должна гарантировать что:

- только персонал, прошедший процедуры идентификации и аутентификации может получать доступ к «ожившим» системам и данным;
- все действия по выходу из нештатной ситуации зафиксированы в виде документа для последующего использования;

- обо всех произведенных действиях руководство было проинформировано в установленном порядке;
- целостность и работоспособность системы подтверждена в минимальные сроки.

Служебные инструкции и ответственность. *Разграничение ответственности путем разделения обязанностей.* Это метод уменьшает риск от случайного или запланированного злоупотребления системой. Разделение зон ответственности между руководителями позволяет уменьшить возможность несанкционированной модификации информации, злоупотребления ею или сервисами. Все критичные операции должны выполняться, как минимум, двумя сотрудниками" - это так называемый принцип «4 глаз». Необходимо учесть следующие моменты:

- действия, которые могут подразумевать сговор (например, покупка товара и контроль закупленного товара), должны быть обязательно разделены;
- если есть опасность сговора, то тогда необходимо применение принципа «4 глаз».

Служебные инструкции и ответственность. *Разделение ресурсов.* Все ресурсы должны быть разделены по целям использования:

- перспективная разработка;
- тестирование (карантин);
- непосредственное осуществление бизнес операций (операционная среда).

Правила переноса нового программного обеспечения в операционную среду должны быть регламентированы.

- операционная среда и среда разработки должны, по возможности, располагаться на разных компьютерах, в разных доменах или директориях;
- среда разработки и карантин должны быть надежно изолированы друг от друга;

- средства разработки, системные редакторы и другие системные утилиты не должны быть доступны в зоне тестирования и операционной среде;
- с целью снижения вероятности возникновения ошибок, для входа в тестовую и рабочую системы должны использоваться разные идентификаторы и пароли, а все меню должны иметь соответствующую маркировку;
- разработчики должны иметь доступ к операционной среде только когда это необходимо для оперативного сопровождения этих систем. Для этого они получают временный доступ, удаляемый по окончании работ.

Защита от вредоносного ПО (вирусов, троянских коней). *Для защиты от вредоносного программного обеспечения должны быть приняты следующие меры:*

- обязательность применения только лицензионного программного обеспечения и запрет использования неутвержденного программного обеспечения должны быть закреплены документально;
- с целью снижения рисков, связанных с получением программного обеспечения через сети общего пользования или на носителях, этот процесс должен быть формализован в виде соответствующего документа;
- все системы должны быть снабжены антивирусным программным обеспечением, которое должно своевременно обновляться. Сканирование всех систем должно проводиться регулярно;
- целостность программного обеспечения, занимающегося обработкой критичных данных (и самих данных) должна проверяться регулярно. По факту;
- отклонения от эталонных значений должно проводиться служебное расследование;
- все точки, через которые в систему поступает информация в виде файлов, сообщений и т.п. должны обеспечивать антивирусный контроль входящей информации;
- в организации должен быть разработан и задокументирован механизм

восстановления после вирусных атак, в частности, определены процедуры резервного копирования программного обеспечения и данных;

- мониторинг всей информации, касающейся вредоносного программного обеспечения, в частности, анализ всех публикуемых бюллетеней и предупреждений по этой теме.

Управление внутренними ресурсами (housekeeping). Резервное копирование информации:

- резервные копии вместе с инструкциями по восстановлению должны храниться в месте, территориально отдаленном от основной копии информации. Для особо важной информации необходимо сохранять три последних копии.
- к резервным копиям должен быть применен адекватный ряд физических и организационных мер защиты, соответствующий стандартам, принятым для используемых носителей;
- носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие сбоев;
- регулярная проверка процедур восстановления и практический тренинг персонала с целью поддержания возможности восстановления данных в установленном порядке и за гарантированный промежуток времени.

Безопасность носителей данных. *Управление съемными носителями:*

- все носители, срок эксплуатации которых истек, должны быть уничтожены в установленном порядке;
- для выноса носителей за пределы организации, должно быть получено специальное разрешение; факт выноса должен быть зафиксирован в специальном журнале (базе данных);
- все носители должны храниться в безопасном месте в соответствии с требованиями компании-производителя.

Хранение и обращение с носителями

1. Хранение в безопасном месте;

2. Следующие носители и информация требуют повышенной безопасности при хранении:
   - бумажные документы: записи на кассетах, копировальная бумага, отчеты, картриджи, магнитные ленты, съемные диски или кассеты, оптические носители, листинги программ, тестовые данные;
   - системная документация.

Процедуры обращения с информацией и ее хранения

- учет и маркировка всех носителей;
- ограничение доступа;
- протоколирование доступа и защита данных из спулинга (которые ожидают распечатки, например).

Безопасность при передаче информации и программного обеспечения. ***Безопасность электронной коммерции*** при обмене информацией:

1. *Аутентификация.* Какой уровень конфиденциальности должны иметь покупатели и продавцы для идентификации друг друга;
2. *Авторизация.* Кто выпустил прайсы и подписаны ли они? Как контрагенты могут это узнать?
3. *Контракт и тендер.* Какие требования для конфиденциальности, целостности, доказательства отправки и приема ключевых документов и отказа от контракта;
4. *Ценовая информация.* Какой уровень доверия может быть применен для целостности рекламного прайс листа и конфиденциальности для скидок;
5. *Порядок расчетов.* Как обеспечивается конфиденциальность и целостность расчетов, платежей, адресатов и подтверждение приема-отправки;
6. *Подтверждение факта оплаты.* Какова степень проверки платежной информации посланной покупателем.

Безопасность электронной почты. При разработке политик необходимо учитывать следующие моменты:

- возможные атаки на электронную почту (например: вирусы, перехват, уничтожение, искажение);

- защита вложений;
- порядок допуска персонала к использованию электронной почты;
- определение ответственности сотрудников за нанесение вреда компании (компрометация имиджа, разглашение коммерческой тайны) в результате использования электронной почты;
- порядок использование криптографии для защиты электронных сообщений;
- архивирование сообщений электронной почты, которые могут в последствии быть предъявлены в качестве доказательств в суде;
- регламентация правил проверки сообщений, которые не могут быть однозначно аутентифицированы.

2. Задание к лабораторной работе:

Изучите следующий сценарий, обсудите и определите вопросы, связанные с реагированием на инцидент, которые следует задавать на каждом этапе процесса реагирования на инцидент. Рассмотрите детали организации и ГРИИБ при формулировании своих вопросов.

Сценарий. *Заражение агента: червь и распределенный отказ в обслуживании (DDoS)*

Этот сценарий касается небольшой семейной инвестиционной компании. Организация имеет только одно местоположение и менее 100 сотрудников. Во вторник утром происходит распространение нового червя через съемные носители, он может скопировать себя, чтобы открыть общие ресурсы Windows. Когда червь заражает хост, он устанавливает DDoS-агента. Через несколько часов после того, как червь начал распространяться, стали доступны антивирусные сигнатуры. Организация уже была подвержена широкому распространению заражения. Инвестиционная фирма наняла небольшую команду экспертов по безопасности, которые часто используют алмазную модель обработки инцидентов безопасности, в некоторых случаях – PDCA-модель.

Подготовка: рассматривает ли организация эту деятельность как инцидент? Если да, то какая из политик организации нарушает эту деятельность?

1. Какие меры предпринимаются для того, чтобы предотвратить повторение подобных инцидентов или ограничить их влияние?

Обнаружение и анализ:

1. Какие предвестники инцидента, если таковые имеются, могут быть обнаружены организацией? Заставят ли какие-либо прекурсоры организацию принять меры до того, как инцидент произошел?
2. Какие показатели инцидента могла бы обнаружить организация? Какие показатели могли бы заставить кого-либо подумать, что инцидент мог произойти?
3. Какие дополнительные инструменты могут понадобиться для обнаружения этого конкретного инцидента?
4. Как бы команда расставила приоритеты в работе с этим инцидентом?

Сдерживание, ликвидация и восстановление:

1. Какую стратегию должна принять организация, чтобы сдержать инцидент? Почему эта стратегия предпочтительнее других?
2. Какие дополнительные инструменты могут потребоваться для реагирования на этот конкретный инцидент?
3. Какой персонал будет задействован в процессах локализации, ликвидации и/или восстановления?
4. Какие источники доказательств, если таковые имеются, должна приобрести организация? Каким образом можно было бы получить доказательства? Где они будут храниться? Как долго они должны храниться?

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Что в себя включает управление коммуникациями и процессами?*
2) *Чего следует придерживаться при безопасности электронной почты?*
3) *Каким образом осуществляется безопасность при передаче информации и программного обеспечения?*
4) *Что включает в себя безопасность электронной коммерции при обмене информацией?*

Лабораторная работа № 7

Тема: Исследование контроля доступа пользователей информационной системы

Цель работы: развитие практических умений и навыков выбора и составления правил разграничения доступа пользователя системы.

1. Теоретические сведения:

Правила контроля доступа:

1. Дифференциация между правилами, которые обязательны или необязательны;
2. Создание правил доступа по принципу "Запрещено все, что не разрешено явно";
3. Определение действий, для осуществления которых нужен администратор.

Управление доступом пользователя. *Регистрация пользователя:*

1. Использование уникального идентификатора пользователя, по которому его можно однозначно идентифицировать. Применение групповых идентификаторов может быть разрешено только там, где это требуется для выполнения работы;
2. Проверка, что пользователь авторизован ответственным за систему для работы с ней. Возможно получение отдельного разрешения для наделения правами пользователя у руководства;
3. Проверка, что уровень доступа соответствует бизнес задачам политике безопасности организации и не противоречит распределению обязанностей (ответственности);
4. Документальная фиксация назначенных пользователю прав доступа;
5. Ознакомление пользователя под роспись с предоставленными правами доступа и порядком его осуществления;
6. Все сервисы должны разрешать доступ только аутентифицированным пользователям;

7. Обеспечение формального списка всех пользователей, зарегистрированных для работы в системе;
8. Немедленное исправление (удаление) прав доступа при изменении должностных обязанностей (увольнении);
9. Периодический контроль и удаление не используемых учетных записей;
10. Обеспечение недоступности запасных идентификаторов другим пользователям.

Управление привилегиями. Многопользовательская система должна иметь следующую формализацию процесса авторизации:

1. Права доступа к каждому системному компоненту (например, ОС, СУБД и приложения) должны быть определены для всех категорий персонала, имеющих к ним доступ;
2. Привилегии индивидуальных пользователей, выдающиеся по мере необходимости или от случая к случаю должны быть минимальны - только такие, какие необходимы;
3. Доступ должен предоставляться лишь после успешного прохождения процессов идентификации и аутентификации. Факт получения доступа должен фиксироваться в системном журнале;
4. Минимизация пользовательских привилегий должна достигаться использованием системных процедур.

Управление паролями пользователей:

1. Все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личного пароля и использования групповых паролей только внутри группы.
2. Рекомендуется настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить.
3. Временные пароли должны передаваться пользователям безопасным образом.

4. Необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой. Пользователь должен подтвердить получение пароля.

Проверка прав пользователей:

1. Проверка прав пользователей должна проводиться регулярно (каждые 6 месяцев) или после каждого изменения в системе;
2. Проверка прав пользователей, имеющих особые привилегии для доступа в систему должна проводиться чаще - каждые 3 месяца;
3. Необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав.

Ответственность пользователей. *Использование паролей.*

Все пользователи должны знать, что необходимо:

1) Хранить пароли строго конфиденциально.
2) Избегать записывать пароли на бумаге, если они не хранятся в безопасном месте.
3) При компрометации (разглашении или подозрении на разглашение пароля) немедленно менять пароли.
4) Выбирать качественные пароли, а именно:
   - длина пароля - не менее 6 символов;
   - пароль легко запоминается;
   - пароль не является легко идентифицируемой информацией (имя пользователя, дата рождения и т.п.);
   - пароль не является повторяющейся последовательностью каких-либо символов (например, "111111", "аааааа" и т.п.).
5) Изменять пароли на регулярной основе (либо через определенный промежуток времени, либо после определенного числа использований), при этом пароли привилегированных пользователей должны меняться чаще. При смене пароля недопустимо выбирать пароли, которые уже использовались ранее.

6) Изменять заданный администратором временный пароль при первом же входе в систему.
7) Не использовать автоматический вход в систему, не применять сохранение пароля под функциональными клавишами.
8) Не сообщать другим пользователям личный пароль, не регистрировать их в системе под своим паролем.

Пользователи должны:

1. Завершать активную сессию перед тем, как отлучиться от оборудования, за исключением случаев длительной автоматической обработки данных при обязательном условии блокировки экрана и клавиатуры.
2. Обязательно завершать соединение с сервером по окончании работы с ним, а не просто выключать терминал или компьютер.
3. Обеспечивать безопасность рабочих станций и терминалов путем блокирования клавиатуры в случае ухода с рабочего места.

Контроль и управление удаленного (сетевого) доступа. *Правила использования сетевых служб и сервисов:*

1. Сети и сетевые службы, к которым возможен доступ;
2. Предоставление доступа к конкретным сетям и сетевым службам только после прохождения процедур идентификации и аутентификации;
3. Порядок осуществления удаленного доступа должен быть регламентировано соответствующими документами (процедуры, регламенты, инструкции).

Контроль доступа в операционную систему. Необходимо обеспечить:

1. Идентификацию и аутентификацию пользователя, а при необходимости и идентификацию оборудования (сетевой адрес, номер терминала и т.п.), с которого осуществляется доступ;
2. Запись успешных и неудачных попыток входа;
3. Использование качественных паролей, если применяется парольная система аутентификации;

4. При необходимости ограничить временные рамки доступа пользователя в систему и число одновременных подключений.

Процедура входа в систему (log on). Процедура должна:

1. Не выдавать информации о типе и версии системы или приложения ("системных баннеров") до успешного завершения процедур идентификации и аутентификации.
2. Выдавать предупреждение, что вход в систему разрешен только авторизованным пользователям.
3. Не выдавать подсказок и справочной информации, чтобы усложнить проникновение в систему неавторизованному пользователю.
4. Проверка введенной информации осуществлять только после полного ее ввода. В случае обнаружения ошибки система не должна уточнять, какие именно данные введены неправильно.
5. Ограничивать число неудачных попыток входа. При этом каждая итерация должна включать:
   - запись неудачной попытки входа;
   - временную задержку перед следующей попыткой входа в систему или блокирование всех дальнейших попыток входа без дополнительной авторизации (как с введением ПИН кода в мобильном телефоне);
   - отсоединение.
6. Контролировать ограничения по времени, заданные для пользователя, и отказывать в доступе при их нарушении.
7. После успешного входа пользователя в систему информировать его:
   - о дате и времени предыдущего входа в систему
   - о любых неуспешных попытках входа, произошедших с момента последней успешной регистрации.

Контроль доступа в операционную систему. *Система управления паролями:*

1. Обязательное применение индивидуальных паролей.

2. По возможности, позволять пользователям выбирать и менять свой пароль, а также предусмотреть процедуры контроля ошибок при вводе пароля.
3. Обязательное (путем применения соответствующей процедуры) применение качественных паролей.
4. В системах, где пользователь должен сам создать свой пароль, обязательно должна присутствовать процедура смены заданного администратором пароля при первом входе в систему.
5. Обеспечить запись старых паролей пользователей (например, за предыдущие 12 месяцев), чтобы предотвратить их повторное использование.
6. Пароль не должен отображаться при вводе.
7. Файл (база данных) паролей должен храниться отдельно от данных прикладных программ.
8. Файл (база данных) паролей должен храниться в защищенном при помощи криптографических методов виде, при этом должны применяться стойкие алгоритмы.
9. Пароли по умолчанию, устанавливаемые производителями оборудования и программного обеспечения, должны быть заменены в обязательном порядке.

Использование системных утилит:

1. Применять процесс аутентификации при использовании системных утилит
2. Раздельно хранить системные утилиты и приложения
3. Ограничить использование системных утилит минимально возможному числу доверенных авторизованных пользователей
4. Специальная авторизация при использовании системных утилит
5. Ограничение доступности системных утилит
6. Протоколирование использования системных утилит
7. Определение и документирование способа авторизации для запуска системных утилит

8. Удаление всех системных утилит, использовании которых в данной системе не является необходимым.

Мониторинг доступа и использования систем. *Мониторинг использования системы.*

Процедуры и места повышенного риска:

- Фиксация в журнале данных о доступе, включая:

1. идентификатор пользователя;
2. дата и время важных (ключевых) событий;
3. тип события;
4. затребованные файлы;
5. использованные программы и утилиты.

- Фиксация в журнале всех привилегированных операций, таких как:

1) вход с правами суперпользователя (администратора);
2) старт и остановка системы;
3) присоединение устройств ввода-вывода.

- Фиксация в журнале всех попыток неавторизованного доступа, таких как:

1) неудачные попытки;
2) нарушения правил политик доступа и уведомления на межсетевой экран;
3) тревоги от систем обнаружения вторжений.

- Фиксация в журнале всех системных предупреждений и неисправностей таких как:

1. консольные уведомления или тревожные сообщения;
2. сбои при ведении системного журнала;
3. тревожные сообщения при сбоях в сетевом управлении.

Мобильные компьютеры и пользователи. *Удаленная работа.*

Требования безопасности:

– Обеспечение физической защиты места удаленной работы, включая физическую безопасность здания или ближайшего окружения;

- Обеспечение безопасности телекоммуникаций, учитывающее необходимость удаленного доступа к внутренним ресурсам компании; важность информации и систем, к которым будет осуществлен удаленный доступ; прохождение через каналы связи;
- Учет возможной угрозы неавторизованного доступа к информации или ресурсам, от иных близких к удаленному пользователю людей, например, семья, друзья.

Обеспечение безопасности:

1) Обеспечение необходимым оборудованием для удаленного мобильного доступа.
2) Определение разрешенных видов работ, разрешенного времени доступа, классификация информации, которая может обрабатываться удаленно, определение систем и сервисов, к которым данному мобильному пользователю разрешен удаленный доступ.
3) Обеспечение необходимым коммуникационным оборудованием, включая средства обеспечения безопасности.
4) Физическая безопасность.
5) Правила доступа к оборудованию и информации для членов семьи и посетителей.
6) Обеспечение программным обеспечением и оборудованием.
7) Наличие процедур резервного копирования и обеспечения непрерывности ведения бизнеса.
8) Аудит и мониторинг безопасности.
9) Аннулирование разрешения, прав доступа и возврат оборудования при отмене (завершении) удаленного мобильного доступа.

2. Задание к лабораторной работе:

1. Для ознакомления с примером составления правил администрирования просмотрите материал приведенный в приложении 1 (см.Приложение).
2. Изучите следующий сценарий. Обсудите и определите меры реагирования на инцидент, которые следует принимать на каждом этапе процесса

реагирования на инцидент. Рассмотрите детали организации и ГРИИБ при формулировке вопросов.

Сценарий: *Несанкционированный доступ к записям заработной платы.*

Этот сценарий касается больницы среднего размера с несколькими дополнительными офисами и медицинскими службами. В организации есть десятки мест, где работают более 5000 сотрудников. Из-за размера организации, они приняли модель CSIRC с распределенными командами реагирования на инциденты. У них также есть координационная группа, которая следит за группой операций по обеспечению безопасности и помогает им общаться друг с другом.

В среду вечером, группа физической безопасности организации получает звонок от администратора фонда заработной платы, который видел, как неизвестный человек покинул ее офис, побежал вниз по коридору и вышел из здания. Администратор оставила ее рабочее место незапертым и осталась без присмотра всего на несколько минут. Программа начисления заработной платы все еще входит в систему и находится в главном меню, как и в тот момент, когда она покинула его, но администратор замечает, что мышь, похоже, была перемещена. Команде, отвечающей за инцидент, было предложено собрать доказательства, связанные с инцидентом, и определить, какие действия были предприняты.

Команды безопасности отрабатывают модель цепочки убийств и понимают, как использовать базу данных VERIS. Для дополнительного уровня защиты они частично передали на внешний подряд штат УСРГ для круглосуточного мониторинга.

Подготовка:

1. Ответы будут варьироваться в зависимости от операционной группы кибербезопасности. Примеры:
2. Считает ли организация эту деятельность инцидентом? Если да, то какая из политик организации нарушает эту деятельность?

3. Какие меры предпринимаются для предотвращения подобных инцидентов или ограничения их последствий?

Выявление и анализ:

1. Какие предвестники инцидента, если таковые имеются, могут быть обнаружены организацией? Заставят ли какие-либо прекурсоры организацию принять меры до того, как инцидент произошел?
2. Какие показатели инцидента могут быть обнаружены организацией? Какие показатели могли бы заставить кого-либо подумать, что инцидент мог произойти?
3. Какие дополнительные инструменты могут понадобиться для обнаружения этого конкретного инцидента?
4. Как бы команда расставила приоритеты в работе с этим инцидентом?

Сдерживание, ликвидация и восстановление:

1. Какую стратегию должна принять организация для сдерживания инцидента? Почему эта стратегия предпочтительнее других?
2. Какие дополнительные инструменты могут потребоваться для реагирования на данный конкретный инцидент?
3. Какой персонал будет задействован в процессах локализации, ликвидации и/или восстановления?

Деятельность после происшествия:

1. Что можно сделать для предотвращения подобных инцидентов в будущем?
2. Что можно сделать, чтобы улучшить обнаружение подобных инцидентов?

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Что Вы понимаете под контролем доступа?*
2) *Как осуществляется мониторинг доступа и использования систем?*
3) *Какую ответственность несут пользователи?*
4) *Управление доступом пользователя.*
5) *Контроль доступа в операционную систему.*

Лабораторная работа № 8

Тема: Процесс разработки и техническая поддержка автоматизированных систем

Цель работы: совершенствование навыков проверки технической поддержки вычислительных систем с защитой на стадии их эксплуатации.

1. Теоретические сведения:

Безопасность приложений. *Проверка входных данных.* Необходимы следующие поверки:

1) Проверка входных данных на следующие ошибки:
   - превышение размерности значения;
   - недопустимые символы во входном потоке;
   - отсутствующие или неполные данные;
   - объем входных данных выше или ниже нормы;
   - запрещенные или неверные управляющие значения.
2) Периодическая проверка целостности и правильности содержимого ключевых полей или файлов данных.
3) Проверка твердых копий входных документов на любые запрещенные (несанкционированные) изменения.
4) Процедуры реагирования на подтвержденные ошибки.
5) Процедуры проверки достоверности входных данных.
6) Определение ответственности для всего персонала, вовлеченного в процесс обработки и ввода исходных данных.

Зоны риска. Риск сбоев процессов и нарушения целостности.

1. Программы с функциями добавления или уничтожения данных;
2. Процедуры по предотвращению некорректного запуска программ после предыдущих сбоев;
3. Применение программ для восстановления после сбоев.

Проверки и средства управления:

1) Контроль сессий и автоматического выполнения заданий на предмет отклонений от обычного использования ресурсов.
2) Контроль изменений использования ресурсов по сравнению с предыдущими:
    a. запусками программ;
    b. изменениями файла;
    c. передачами управления от программы к программе;
3) Проверка правильности сгенерированных системных данных.
4) Проверка целостности данных и программного обеспечения после их передачи с одного компьютера на другой.
5) Общая контрольная сумма (хеш) всех записей и файлов.
6) Проверка того, что программы запускаются в соответствующее время.
7) Проверка того, что программы запускаются в соответствующем режиме и останавливаются в случае неисправностей, а также что связанные процессы останавливаются до устранения всех проблем.

Проверка выходных данных:

1) Проверка правильности и смысла выходных данных.
2) Проверка всех контрольных точек, чтобы убедиться, что все данные были обработаны.
3) Предоставление системе обработки информации всех необходимых данных для определения правильности, полноты, точности и класса информации.
4) Процедуры для проверки правильности выходной информации.
5) Определение ответственности для всего персонала, вовлеченного в процесс обработки выходных данных.

Криптографические средства управления. *Политика использования средств криптографической защиты.* При разработке политики необходимо учесть:

- управленческий подход к использованию СКЗИ внутри организации, включая основные принципы, какие именно классы информации должны быть защищены;
- политика управления ключами, включая методы для восстановления зашифрованной информации в случае утери, компрометации или уничтожения ключей;
- распределение обязанностей: кто и за что несет ответственность;
- внедрение политики;
- управление ключами;
- порядок определения адекватного уровня криптографической защиты;
- стандарты, которые могут быть внедрены и адаптированы в организации (какие решения подходят для каких бизнес процессов).

Стандарты, процедуры, методы:

1) Генерация ключей для разных криптосистем и разных приложений.
2) Генерация и получение открытых ключей.
3) Выдача ключей пользователям, включая процедуру активации ключа после его получения.
4) Хранение ключей, включая порядок получения авторизованными пользователями доступа к ключам.
5) Порядок смены ключей.
6) Действия в случае компрометации ключей.
7) Отзыв ключей, включая порядок их деактивации при компрометации или увольнении ответственного за них сотрудника, а также определение случаев, когда эти ключи должны быть сохранены.
8) Восстановление поврежденных или утерянных ключей (как часть управления непрерывностью бизнеса).
9) Архивирование и резервное копирование ключей.
10) Уничтожение ключей.
11) Протоколирование всех действий, связанных с управлением ключами.
12) Ограничение срока действия ключей.

Безопасность системных файлов.

I. Контроль объектов операционной системы:

- обновление библиотек должно выполняться только с разрешения руководства;
- если возможно, ОС должна содержать только исполняемые файлы;
- исполняемые файлы и изменения библиотек не должны внедряться в ОС до подтверждения их успешного тестирования, а также информирования и обучения пользователей (если в этом нет острой необходимости);
- после всех изменений в библиотеках должна быть обеспечена проверка всех регистрационных журналов;
- предыдущие версии должны быть сохранены для непредвиденных случаев.

II. Защита данных, полученных в результате тестов систем:

1. Система разграничения доступа к тестовой системе должна соответствовать доступу к обычной системе.
2. Необходимо обеспечение разных (раздельных) авторизаций каждый раз, когда рабочая (оперативная) информация копируется в тестовую систему.
3. Рабочая информация должна быть немедленно удалена из тестовой системы после завершения тестов.
4. Копирование и использование рабочей (оперативной) информации должно быть запротоколировано для последующей возможности аудита.

III. Контроль доступа к исходным текстам программ и библиотек:

1. Где возможно, исходные тексты программ не должны содержаться в ОС;
2. Для каждого приложения должен быть назначен ответственный сотрудник, отвечающий за контроль исполняемых модулей;
3. Персонал из службы поддержки не должен иметь неограниченный доступ к исходным текстам программ и библиотек;
4. Изменения и дополнения в исходные тексты программ и библиотек, а также передача исходных текстов программистам должна осуществляться только вместе с библиотеками и по разрешению менеджера поддержки данного приложения;

5. Листинги программ должны храниться в безопасном месте;
6. Все попытки осуществления доступа к исходным текстам должны протоколироваться;
7. Старые версии исходных текстов программ должны быть заархивированы, с отметкой времени и даты и вместе со всем сопутствующим программным обеспечением, процедурами, описаниями и т.д.;
8. Поддержка и копирование исходных текстов библиотек и программ должны быть предметом процедур контроля изменений.

Безопасность процессов разработки и поддержки. *Процедуры контроля изменений:*

- документальное закрепление типовых уровней доступа;
- обеспечение, того, что изменения сделаны авторизованными пользователями;
- идентификация всего программного обеспечения, информации, баз данных, аппаратного обеспечения, которое требует изменений;
- получение формального разрешения для детализации предложений до начала работ;
- обеспечение того, что авторизованные пользователи принимают (проверяют) изменения до их внедрения;
- обеспечение безопасного внедрения изменений без последствий для бизнеса;
- обеспечение изменений системной документации после каждой модификации, а также архивация старой документации или ее отклонение;
- обеспечение контроля версий для всех обновлений программного обеспечения;
- обеспечение протоколирования всех запросов на изменение;
- обеспечение соответствующих изменений оперативной и пользовательской документации.

– обеспечение того, что внедрение изменений имело место в соответствующее время и не затронуло вовлеченные в процесс бизнес процессы.

Технический обзор изменений в операционных системах. *После внесения изменений в ОС необходимо осуществить анализ важных приложений и целостности процедур* (необходимо убедиться в их работоспособности):

1. убедиться, что годовой план поддержки систем и бюджет покроет расходы на анализ и тестирование систем после изменений ОС;
2. убедиться, что уведомление об изменениях в ОС пришло вовремя, что позволило сделать необходимый анализ перед внедрением изменений;
3. убедиться, что соответствующие изменения внесены в планы обеспечения непрерывности бизнеса.

2. Задание к лабораторной работе:

Сценарий: Исходящие DDoS атаки

В воскресенье вечером один из датчиков обнаружения вторжения в сеть организации оповещает о подозрении на исходящую DDoS активность, связанную с большим количеством пинговых сигналов протокола Internet Control Message Protocol (ICMP). Аналитик вторжения просматривает предупреждения; хотя аналитик не может подтвердить, что предупреждения точны, они не совпадают ни с какими известными ложными срабатываниями. Аналитик связывается с группой реагирования на инцидент, чтобы продолжить расследование. Поскольку DDoS активность использует поддельные IP-адреса источника, требуется значительное время и усилия, чтобы определить, какой хост или узлы в организации его производят; тем временем, DDoS активность продолжается. Исследование показывает, что пять серверов генерируют трафик DDoS. Анализ пяти серверов показывает, что каждый из них содержит признаки руткита DDoS. Кроме того, три из этих серверов, судя по всему, использовались для атаки на другие внутренние хосты, а один, судя по всему, использовался и для атаки на внешние хосты.

Вопросы для этого сценария:

1. Как бы команда определила, какие хосты в организации производят трафик? Какие другие команды могут помочь команде реагирования на инцидент?
2. Свяжется ли организация с владельцами IP-адресов, на которые была направлена DDoS-атака? Если да, то кто будет с ними связываться и как этот контакт будет осуществляться?
3. Если команда реагирования на инцидент определит, что первоначальная компрометация была выполнена через модем на одном из серверов, как команда будет продолжать расследование этой деятельности?

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Что означает безопасность приложений?*
2) *Для чего используют криптографию при разработке приложений?*
3) *Что включает в себя безопасность процессов разработки и поддержки?*
4) *Если команда реагирования на инцидент определит, что первоначальная компрометация была выполнена через модем на одном из серверов, как команда будет продолжать расследование этой деятельности?*

Лабораторная работа № 9

Тема: Исследование процесса управления непрерывностью бизнеса

Цель работы: закрепление навыков планирования и управления непрерывностью бизнеса при инцидентах ИБ.

1. Теоретические сведения:

Процесс управления непрерывным ведением бизнеса включает в себя:

1. Осознание рисков, их вероятностей, возможных последствий, включая идентификацию и расстановку приоритетов для критичных бизнес процессов.
2. Осознание ущерба в случае прерывания бизнеса и создание бизнес целей для информационно-обрабатывающей системы компании.
3. Выбор подходящей схемы страхования, которая может являться одной из форм поддержки непрерывности ведения бизнеса.
4. Формализация и документирование стратегии ведения непрерывного бизнеса, содержащей согласованные цели бизнеса и приоритеты.
5. Регулярное тестирование и обновление планов и процессов.
6. Необходимо убедиться, что управление непрерывным ведением бизнеса внедрено в организационные процессы и структуру компании.
7. Ответственность для координации управления непрерывным ведением бизнеса должна быть распространена по соответствующим уровням внутри организации, так называемый форум по информационной безопасности.

Создание и внедрение плана непрерывности бизнеса должно заключаться в следующем:

1. Распределение ответственности и определение всех контр аварийных процедур (порядок действий в аварийной ситуации).
2. Внедрение контр аварийных процедур для восстановления систем в отведенный период времени. Особое внимание уделяется оценке зависимости бизнеса от внешних связей.
3. Документирование всех процессов и процедур.

4. Соответствующее обучение персонала порядку действий в аварийных ситуациях включая управление в кризисных процессах.
5. Тестирование и обновление планов.

Основы планирования непрерывности бизнеса:

- условия вступления в действие планов (как оценить ситуацию, кто в нее вовлечен);
- контраварийные процедуры, описывающие действия в случае инцидентов, представляющих опасность для бизнес операций или/и человеческой жизни. Процедуры должны включать в себя мероприятия по связям с общественностью и органами власти;
- процедуры нейтрализации неисправностей, в которых описываются действия по выведению жизненно важных бизнес нужд или служб поддержки во временное альтернативное помещение и возвращение их в соответствующий период времени;
- процедуры восстановления, в которых описаны действия по возвращению к нормальному процессу бизнес операций;
- разработка программы, в которой описаны, как и когда план будет протестирован и процесс внедрения этого плана;
- действия по информированию и обучению, которые разрабатываются для понимания персоналом процесса обеспечения непрерывности бизнеса и гарантии, что этот процесс продолжает быть эффективным;
- личная ответственность - кто именно отвечает за выполнение каждого компонента плана, с указанием дублирующих лиц.

Тестирование планов обеспечения непрерывности бизнеса:

1. *Базовые тесты различных сценариев* (обсуждение мероприятий по восстановлению бизнеса в случае различных ситуаций).
2. *Моделирование* (практический тренинг персонала по действиям в критичной ситуации).
3. *Тестирование технических мероприятий по восстановлению* (для гарантии того, что информационная система будет эффективно восстановлена).

4. *Тестирование технических мероприятий по восстановлению в альтернативном месте* (запуск бизнес процессов вместе с восстановительными мероприятиями вне основного места расположения).
5. *Тесты систем и поставщиков услуг* (гарантия, что внешние предоставляемые сервисы и продукты будут соответствовать контрактным обязательствам).

Комплексные учения (тестирование того, что компания, персонал, оборудование, информационная система могут справиться с нештатной ситуацией).

2. Задание к лабораторной работе:

1. Сформулируйте краткий план управления непрерывностью бизнеса. Проект предоставьте в удобном для вас виде (текстовое описание, схема, презентация, видео, рисунок и т.п.)
2. ***Сценарий**: Загрузка инструмента для взлома*

В пятницу днем датчик обнаружения сетевого вторжения записывает подозрительную FTP-активность с участием внутреннего пользователя, загружающего файлы с внешнего FTP-сервера. Аналитик вторжения просматривает предупреждения и замечает, что они являются ложными срабатываниями. Хотя предупреждения указывают на то, что произошла атака, поддерживающие данные, записанные датчиком, не показывают никаких признаков атаки. Однако данные вызывают другие опасения, так как они показывают, что пользователь загружает исполняемые файлы из подозрительной структуры каталога, содержащей повторяющиеся пробелы и периоды, а также символы, которые обычно не видны в именах каталогов FTP. Аналитик вторжения использует поисковую систему в Интернете для поиска дополнительной информации об именах исполняемых файлов, и некоторые из них совпадают с именами хакерских инструментов. Аналитик связывается с командой реагирования на инциденты для проведения дальнейшего анализа и определения того, как эта деятельность должна быть обработана.

Дополнительные вопросы для этого сценария:

1. Как бы команда определила, какие файлы были загружены пользователем?

2. Как бы команда подтвердила, что загруженные файлы являются инструментами для взлома?

3. Чем бы отличалась работа с этим инцидентом, если бы пользователь, подозреваемый в загрузке инструментов, был членом команды информационной безопасности организации?

4. Чем бы отличалась работа с этим инцидентом, если бы пользователь, подозреваемый в загрузке инструментов, был членом группы реагирования на инцидент?

5. Чем бы отличалась процедура рассмотрения этого инцидента, если бы пользователь, подозреваемый в загрузке инструментов, был подрядчиком, который только что узнал о том, что его контракт не продлевается?

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Создание и внедрение плана непрерывного ведения бизнеса.*
2) *Основы планирования непрерывности бизнеса.*
3) *Тестирование, обеспечение и переоценка плана непрерывного ведения бизнеса.*

Лабораторная работа № 10

Тема: Выявление соответствия системы основным требованиям

Цель работы: совершенствование навыков проектирования информационной системы в соответствии с основными требованиями защиты приложений.

1. Теоретические сведения:

Соответствие требованию законодательства. *Копирайт на ПО:*

1. Разработка и внедрение политики соблюдения авторского права на программное обеспечение, где определяется легальное использование ПО и информационных продуктов.
2. Выпуск стандартов для процедур приобретения программного обеспечения.
3. Обеспечение осведомленности пользователей об авторских правах на программное обеспечение, правилах приобретения программного обеспечения и уведомление пользователей, что в случае нарушения будут предприняты дис-циплинарные действия.
4. Обеспечение возможности доказательства, что данное программное обеспечение лицензионно (лицензии и т.д.)
5. Контроль того, что максимальное число пользователей в лицензии не превышено.
6. Выполнение проверок, что только разрешенные и лицензионные продукты инсталлированы.
7. Разработка политики для обеспечения соответствующих условий лицензионного соглашения.
8. Разработка политики для размещения или передачи программного обеспечения сторонним лицам или компаниям.
9. Применение соответствующих средств аудита.
10. Соблюдение условий для программного обеспечения и информации, полученных из открытых сетей.

Соответствие требованию законодательства. Предотвращение злоупотреблений при работе с автоматизированной системой организации. Автоматизированная система организации создана для выполнения бизнес задач. Любое использование системы для решения задач отличных от основной цели недопустимо. В случае обнаружения системами слежения такого несоот-ветствующего использования системы, необходимо предусмотреть дисциплинарные методы воздействия.

Легальность мониторинга использования информационной системы компании варьируется от страны к стране, поэтому необходимо внесение соответствующих разделов в трудовой договор с сотрудником. Прежде чем внедрить систему мониторинга необходимо проконсультироваться у юриста.

Во многих странах есть законодательство против компьютерных злоупотреблений. Необходимо чтобы пользователи знали, что именно им разрешено делать в информационной системе. Пользователь должен подписать соответствующий документ, регламентирующий порядок его работы в *системе.*

Сохранение улик (свидетельств, доказательств). *Правила обращения с уликами:* степень допустимости улики, когда и при каких условиях она может быть использована в суде в качестве доказательства.

1. *Вес улики:* качество и полнота улики
2. *Адекватность улики.* Подсистема регистрации работает корректно и непрерывно; осуществляется запись всей информации; в любой момент можно получить необходимые сведения (улику) из регистрационных журналов.

2. Задание к лабораторной работе:

1) Составьте таблицу, в которой будут приведены меры соответствия требованиям системного аудита.
2) Просмотрите примеры приведенные ниже. Какой из вариантов показывает, как можно скрыть вредоносное ПО? Аргументируйте свой ответ.

- Хакер использует методы для улучшения рейтинга сайта, чтобы пользователи перенаправлялись на вредоносный сайт.
- Атака запускается против публичного веб-сайта интернет-магазина с целью блокирования его реакции на посетителей.
- Бот-сеть зомби переносит личную информацию обратно к хакеру.
- Сотрудникам организации отправляется электронное письмо с вложением, похожим на антивирусное обновление, но на самом деле вложение состоит из шпионских программ.

Структура отчёта:

Отчет о лабораторной работе оформляется в рабочей тетради либо в печатном виде на листах формата А4. Отчет должен содержать:

2.1. Задание по лабораторной работе.

2.2. Решение задачи (выполнение задания).

2.3. Ответы на контрольные вопросы.

2.3. Краткие выводы по лабораторной работе.

Контрольные вопросы:

1) *Поясните соответствие требованиям законодательства.*
2) *В чем должно заключаться соответствие политике безопасности?*
3) *Важность и необходимость процедуры мониторинга информационной системы для процесса защиты данных.*
4) *Какова роль сохранности свидетельств при расследовании инцидентов информационной безопасности.*

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Президента Республики Узбекистан №ПП-4996 от 17.02.2021 года «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта». Эл.ресурс: https://lex.uz/docs/5297051.
2. Постановление Президента Республики Узбекистан №ПП-4452 от 14.09.2019 года «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты». Эл.ресурс: https://lex.uz/docs/4665551.
3. ПРИЛОЖЕНИЕ № 1 к Указу Президента Республики Узбекистан № УП-4947 от 7.02.2017 года «СТРАТЕГИЯ ДЕЙСТВИЙ по пяти приоритетным направлениям развития Республики Узбекистан в 2017 - 2020 годах». Эл.ресурс: https://lex.uz/docs/3107042.
4. Н.Г.Милославская, М.Ю.Сенаторов, А.И.Толстой, Управление инцидентами информационной безопасности и непрерывностью бизнеса, Горячая линия – Телеком, Москва, 2015.
5. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».
6. O'z DSt ISO/IEC 27035:2015 «Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами».
7. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем: Учеб.для вузов / В 2 томах. Том 1: Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая линия–Телеком, 2014.
8. Шангин В.Ф., «Информационная безопасность и защита информации», Учебное пособие. М.: ДМК. 201. 702 с.
9. Платонов В.В. Программно-аппаратные средства защиты информации. М.:Academia. 2013. 336 с.
10. Karen Kent, Suzanne Chevalier, Hung Dang, NIST Special Publication 800-86 Guide to integrate forensic techniques into incident response, Gaithersburg, 2006.

СОДЕРЖАНИЕ

ПРИЛОЖЕНИЕ 1

Пример правил администрирования:

Цель: ввести правила администрирования и внедрить правила информационной безопасности.

Инструктаж пользователей:

Цель: обеспечить знание и понимание всеми пользователями правил.

Правило: все пользователи сетей и систем Компании должны пройти инструктаж для ознакомления с правилами безопасности, прежде чем им будет предоставлен доступ. Пользователи, которые уже работают в сети, должны пройти инструктаж в течение 30 дней после введения в действие этих правил.

Публикация и уведомление:

Цель: опубликовать правила, чтобы они стали доступными для всех пользователей, и сообщить им о публикации.

Правило: отдел кадров несет ответственность за публикацию во внутренней сети Компании правил информационной безопасности и всех их обновлений. Отдел кадров должен уведомить каждого пользователя о публикации документа правил, а также о том, как получить к ним доступ.

Цель: предоставить печатные копии тем, кто не имеет доступа к электронной версии документа.

Правило: отдел кадров должен предоставить каждому отделу и пользователям, не имеющим права доступа во внутреннюю сеть, по одной печатной копии документа правил одновременно с публикацией электронной версии.

Обязанности руководства:

Цель: Предоставить право на проведение мониторинга.

Правило: Руководство имеет право контролировать всю деятельность в системах и сетевой трафик для обеспечения гарантий выполнения этих правил. Для этого руководство назначает соответствующих администраторов

и возлагает на них обязанности по проведению мониторинга, а также другие обязанности, связанные с поддержкой безопасности.

Цель: предоставить право устанавливать средства управления доступом.

Правило: руководство имеет право устанавливать средства управления доступом в соответствии с требованиями этих правил.

Цель: предоставить право тестирования средств управления доступом.

Правило: руководство и назначенные администраторы несут ответственность за тестирование средств управления доступом и сети на наличие уязвимых мест. Пользователи не должны проводить тестирование на наличие уязвимых мест в сети и средств управления доступом вручную или с помощью программных средств.

Цель: исключит возможность использования уязвимых мест.

Правило: когда уязвимые места становятся известны, пользователи не должны использовать их возможности вручную или с помощью программных средств.

Цель: Ограничить пользование средствами обеспечения безопасности и тестирования только представителями руководства и администраторами.

Правило: Руководство и назначенные администраторы должны иметь доступ к средствам, которые могут помочь в управлении и тестировании системы обеспечения информационной безопасности. Пользователи не должны иметь доступ к этим средствам через сеть Компании. Пользователи не должны загружать эти средства в любую область сети или "скачивать" их оттуда.

Обязанности администраторов:

Цель: обязать администраторов сохранять важные записи, фиксирующие нарушения безопасности.

Правило: администраторы безопасности и системные администраторы должны делать записи обо всех нарушениях безопасности. Эти записи должны быть достаточно подробны, чтобы их можно было использовать для наложения дисциплинарных взысканий и при доработке правил безопасности.

Цель: обязать использовать журналы допустимых рисков в качестве утвержденной правилами безопасности процедуры разрешенного нарушения этих правил.

Правило: администраторы безопасности должны вносить каждое разрешенное нарушение правил в журналы допустимых рисков. Руководители, которым необходимо нарушить отдельные предписания этих правил, должны расписаться в таком журнале и, тем самым, взять на себя ответственность за безопасность систем и сетей.

Цель: установить, что только системные и сетевые администраторы могут создавать и поддерживать идентификационные реквизиты пользователей и информацию, обеспечивающую управление доступом.

Правило: системные и сетевые администраторы должны быть назначены ответственными за работу с информацией о пользователях и средствах управления доступом. В эти обязанности необходимо включить создание и модификацию учетных записей пользователей, а также, при необходимости, внесение изменений в средства управления доступом.

Цель: установить проведение полугодового аудита идентификационных реквизитов пользователей и средств управления доступом.

Правило: системные администраторы и администраторы безопасности должны один раз в полгода проводить аудит учетных записей пользователей и соответствующих средств управления доступом для обеспечения их пригодности к использованию.

Цель: обязать администраторов разработать процедуры регистрации определенных функций систем и сетей.

Правило: системные, сетевые администраторы, а также администраторы безопасности должны определить, какую информацию необходимо сохранять в системных и сетевых журналах. Кроме того, необходимо регистрировать все важные действия в области обеспечения безопасности.

Цель: обязать регулярно анализировать содержимое различных журналов регистрации и назначить администраторов, которым будет предоставлено исключительное право просматривать журналы.

Правило: только уполномоченные администраторы должны регулярно просматривать системные и прочие журналы регистрации.

Цель: обеспечить защиту различных журналов регистрации.

Правило 1: администраторы должны предпринять необходимые меры предосторожности, чтобы исключить отключение заполнения журналов, их исправление или удаление.

Правило 2: обеспечить гарантии своевременной отчетности администраторов о нарушениях защиты.

Правило 3: при обнаружении нарушений этих правил или безопасности сетей администраторы должны выполнить установленные процедуры.

Цель: обеспечить создание резервных копий и архивирование системных журналов.

Правило: администраторы должны дублировать активные регистрационные журналы на онлайновые запоминающие устройства. Онлайновая копия должна быть заархивирована и перенесена на автономное запоминающее устройство в последний день каждого месяца. Автономное запоминающее устройство, на котором хранятся журналы, должно обслуживаться в течение двух лет, если в договоре или предписаниями судебных органов не установлен более длительный срок хранения.

Правовые санкции и отчетность об инцидентах:

Цель: установить, что каждый отвечает за реализацию этих правил.

Правило: все пользователи должны нести ответственность за внедрение и реализацию положений этих правил, а также связанных с ними процедур. О нарушениях этих правил и процедур необходимо составлять отчеты, пользуясь утвержденными для выполнения этой работы процедурами.

Цель: ввести программу мониторинга различных сообщений об инцидентах, связанных с информационной безопасностью, и об ошибках в программном обеспечении.

Правило: администраторы должны отслеживать широковещательные публикации организаций, сообщающие об инцидентах, ошибках и других проблемах, которые могут повлиять на безопасность сети и систем организации. В список этих организаций должны входить, но крайней мере, две ведущие организации из перечня поставщиков информационных систем, используемых в организации, а также выбранный организацией поставщик антивирусного программного обеспечения.

Цель: установить процедуры взаимодействия с правоохранительными органами.

Правило: меры реагирования на нарушения закона необходимо координировать с руководством. Руководство должно выступать в роли ведущего собственного следователя, а также нести ответственность за связи и взаимодействие с правоохранительными органами.

Цель: ужесточить требования к работе с доказательствами нарушений безопасности.

Правило: данные, необходимые для обработки информации о нарушениях информационной безопасности и об инцидентах, должны сохраняться, чтобы их можно было использовать во время анализа правил информационной безопасности на эффективность применения.

Дисциплинарные меры:

Цель: установить нормы поведения для работающих в сети и с системами Компании.

Правило: категорически запрещено любое поведение, которое неблагоприятно отражается на работе других лиц в системах и сетях Компании, или которое может навредить другим лицам.

Цель: утвердить право руководства отменять право доступа к системам и сети для тех, кто нарушает эти правила.

Правило: руководство имеет право аннулировать любые привилегии доступа пользователей и в любой момент разорвать с ними трудовое соглашение за нарушения предписаний правил безопасности или за поведение, мешающее нормальной работе сети и компьютерных систем Компании.

Цель: утвердить право руководства разрывать соглашения и контракты с теми, кому предоставлено право доступа к системам и сети на основании этих соглашений, если они нарушили эти правила.

Правило: руководство имеет право разорвать контракты и договоры с подрядчиками и другими внешними пользователями, если они нарушают предписания правил или демонстрируют поведение, которое мешает нормальной работе сети и компьютерных систем Компании.

Цель: утвердить право руководства докладывать о нарушениях закона в соответствующие правоохранительные организации.

Правило: руководство имеет право применить собственные меры наказания вместо соответствующих санкций по криминальному или гражданскому законодательству против любого, кто использует, злоупотребляет или атакует сеть организации и информационные системы таким образом, что это может быть отнесено к нарушениям закона и предписаний этих правил.

Методическое пособие к лабораторным работам
по предмету "Инциденты атак и реагирование на них"
для студентов бакалавриата направления образования
5330300 – "Информационная безопасность"

Рассмотрено и рекомендовано к печати
на заседании кафедры "ОИБ"
2021 год 10 03
протокол № 14

Рассмотрено и рекомендовано к печати
на заседании учебно-методического совета
факультета "ИБ"
2021 год 24 03
протокол № 8

Рассмотрено и рекомендовано к печати
на заседании учебно-методического совета
ТУИТ им.Мухаммада ал-Хоразмий
2021 год 27 04
протокол № 9(134)

Составители: А.А. Абдурахманов
З.И. Азизова

Рецензенты: М.М. Кадиров
Х.К. Самаров

Главный редактор: А.А. Ганиев

Корректировщики: У.Т. Алиев
С.Х. Абдуллаева