МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«Менеджмент инцидентов информационной безопасности»
для студентов направления подготовки
10.04.01 Информационная безопасность

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Лабораторная работа №1

Основные направления политики обеспечения информационной безопасности

Цель работы – исследовать основные направления политики обеспечения информационной безопасности.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

1. Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.

2. Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.

3. Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

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).

Правовые (законодательные)

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.

Морально-этические

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. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей и обслуживающего персонала АС.

Технологические

К данному виду мер защиты 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 та-

ких 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

Организационные меры зашиты - 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[1].

Меры физической защиты

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

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.

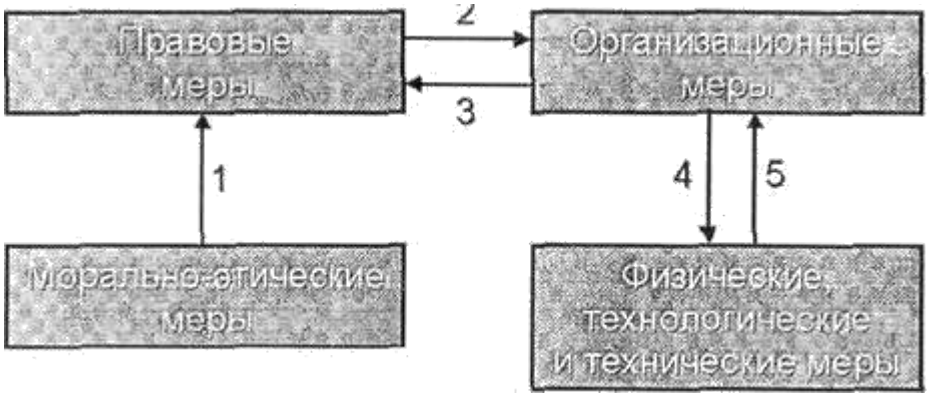

Рисунок 1 – Взаимосвязь мер обеспечения информационной безопасности

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.

Отчеты о событиях и инцидентах информационной безопасности

Рекомендации по заполнению

Назначением данной формы (формы отчета о событиях и инцидентах ИБ) является обеспечение информацией о событии ИБ, а затем, 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 ка-

тегорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения или 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, 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 ГРИИБ. Независимо от того, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена[2].

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.

Отчет о событии информационной безопасности

Дата события

Номер события*: Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

---

* Номера событий назначаются руководителем ГРИИБ организации.

Информация о сообщающем лице

Фамилия		Адрес	
Организация			
Телефон		Электронная почта	

Описание события ИБ

Описание события:

Что произошло

Как произошло

Почему произошло

Пораженные компоненты

Негативное воздействие на бизнес

Любые идентифицированные уязвимости

Подробности о событии ИБ

Дата и время наступления события

Дата и время обнаружения события

Дата и время сообщения о событии

Закончилось ли событие? (отметить в Да Нет квадрате)

Если "да", то уточнить длительность события в днях/часах/минутах

Отчет об инциденте информационной безопасности

Дата инцидента

Номер инцидента*: Соответствующие идентификационные

номера событий и (или) инцидентов (если требуется):

---

* Номера инцидентов назначаются руководителем ГРИИБ организации и привязываются к номеру(ам) соответствующих событий.

Информация о сотруднике группы обеспечения эксплуатации

Фамилия		Адрес	
Телефон		Электронная почта	

Информация о сотруднике ГРИИБ

Фамилия		Адрес	
Телефон		Электронная почта	

Описание инцидента ИБ

Дополнительное описание инцидента:

Что произошло

Как произошло

Почему произошло

Пораженные компоненты

Негативное воздействие на бизнес

Любые идентифицированные уязвимости

Подробности об инциденте ИБ

Дата и время возникновения инцидента

Дата и время обнаружения инцидента

Дата и время сообщения об инциденте

Закончился ли инцидент? (отметить в Да Нет квадрате)

Если "Да", то уточнить длительность инцидента в днях/часах/минутах. Если "Нет", то уточнить, как долго он уже длится

Отчет об инциденте информационной безопасности

Тип инцидента ИБ

(Сделать отметку в одном из квадратов, затем заполнить ниже соответствующие поля)	Действительный	Попытка	Предполагаемый
(Один из) Хищение (ТН)	Намеренная	(указать типы угрозы) Хакерство/логическое про-	

никновение

(HA)

Мошенничество (FR)

Неправильное использование ресурсов

(MI)

Саботаж/физический ущерб (SA)

Вредоносная программа (MC)

Другой ущерб (OD)

Определитель:

(Один из) Случайная

(указать типы угрозы)

Отказ аппаратуры (HF)

Другие природные события

Отказ ПО (SF)

(NE)

Отказ системы связи (CF)

Определить:

потеря значимых сервисов

Пожар (HE)

(LE)

Наводнение (FL)

недостаточное кадровое обес-

(Один из) Ошибка

печение (SS)

Операционная ошибка (OE)

Другие случаи (OA)

Ошибка в эксплуатации аппаратных средств (HE)

Ошибка в эксплуатации ПО (SE)

Неизвестно

Определить:

(указать типы угрозы)

Ошибка пользователя (UE)

Ошибка проектирования (DE)

Другие случаи (включая ненамеренные ошибки) (OA)

Определить:

(Если еще не установлен тип

инцидента ИБ (намеренный, случайный, ошибка), то следует сделать отметку в квадрате "неизвестно" и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)

Определить:

Отчет об инциденте информационной безопасности

Поражение активы

Пораженные активы (при наличии)	(Дать описания активов, пораженных инцидентами ИБ или связанных с ним, включая (где требуются), серийные, лицензионные номера и номера версий)
	Информация/данные
	Аппаратные средства
	Программное обеспечение
	Средства связи
	Документация

Негативное воздействие/влияние инцидента на бизнес

Сделать отметку в соответствующих квадратах для указанных ниже нарушений, затем в колонке "значимость" указать степень негативного воздействия на бизнес по шкале 1 10, используя следующие сокращения (указатели категорий): (FD) - финансовые убытки/разрушение бизнес-операций, (CE) - коммерческие и экономические интересы, (PI) - информация, содержащая персональные данные, (LR) - правовые и нормативные обязательства (это необходимо

сравнить с английским оригиналом), (MO) - менеджмент и бизнес-операции, (LG) - потеря престижа (см. примеры в приложении В). Записать кодовые буквы в колонке "указатели", а если известны действительные издержки, - указать их в колонке "стоимость".

	Значимость	Указатели	Издержки
Нарушение конфиденциальности (то есть несанкционированное раскрытие)			
Нарушение целостности (то есть несанкционированная модификация)			
Нарушение доступности (то есть недоступность)			
Нарушение неотказуемости			
Уничтожение			

Общие расходы на восстановление после инцидента ИБ

	Значимость	Указатели	Издержки
(Там, где возможно, необходимо указать общие расходы на восстановление после инцидента ИБ в целом по шкале 1 10 для "значимости" и в деньгах для "стоимости")			

Отчет об инциденте информационной безопасности

Разрешение инцидента

Дата начала расследования инцидента ИБ

Фамилия(ии) лица (лиц), проводившего(их) расследование инцидента

Дата разрешения инцидента ИБ

Дата окончания воздействия

Дата завершения расследования инцидента ИБ

Место хранения отчета о расследовании

Причастные к инциденту лица/нарушители

(Один из)

Лицо (PE)

Организованная группа (GR)

Легально учрежденная организация/учреждение (OI)

Случайность (AC)

Отсутствие нарушителя (NP)
Например, природные факторы, отказ оборудования, человеческий фактор

Описание нарушителя

Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода (CG)

Политика/терроризм (PT)

Развлечения/хакерство (PH)

Месть (RE)

Другие мотивы (OM)

Определить:

Действия, используемые для разрешения инцидента ИБ

(например, "никаких действий", "подручными средствами", "внутреннее расследование", "внешнее расследование с привлечением…")

Действия, запланированные для разрешения инцидента

(включая возможные приведенные выше действия)

Прочие действия

(например, по-прежнему требуется проведение расследования, но другим персоналом)

Отчет об инциденте ИБ

Заключение

(Сделать отметку в одном из квадратов, является ли инцидент значительным или нет, и приложить краткое изложение обоснования этого заключения)	Значительный	Незначительный
(Указать любые другие заключения)		

Оповещенные лица/субъекты

(Эта часть отчета заполняется соответствующим	Руководитель службы ИБ	Руководитель ГРИИБ

лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации)

Местный руководитель (уточнить, какого подразделения)

Руководитель информационных систем

Автор отчета

Руководитель автора отчета

Полиция

Другие лица

(например, справочная служба, отдел кадров, руководство, служба внутреннего аудита, регулятивный орган, сторонняя КСБР)

Определить:

Привлеченные лица

Инициатор	Аналитик	Аналитик
Подпись _____	Подпись _____	Подпись
Фамилия _____	Фамилия _____	Фамилия

Должность Должность Должность

Дата	Дата	Дата
Аналитик	Аналитик	Аналитик
Подпись	Подпись	Подпись
Фамилия	Фамилия	Фамилия
Должность	Должность	Должность
Дата	Дата	Дата

Контрольные вопросы:

1. Определение информационной безопасности, перечень ее составляющих

2. Краткое разъяснение политики безопасности, принципов ее построения и стандартов в этой области.

3. Подробный перечень документов, которые должны быть изданы вместе с политикой безопасности.

Лабораторная работа №2

Организационные меры по обеспечению безопасности

Цель работы – исследовать организационные меры по обеспечению безопасности.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

Форум по информационной безопасности

Разделы форума посвящены следующим вопросам:

1. Обсуждение вносимых в политику изменений, принятие новой версии политики, согласование списков ответственных лиц;

2. Отслеживание и анализ важных изменений в структуре информационных ресурсов компании на предмет выявления новых угроз;

3. Изучение и анализ инцидентов с безопасностью;

4. Принятие важных инициатив по усилению мер безопасности

Форум по координации вопросов, связанных с внедрением средств обеспечения информационной безопасности

а) Выработка соглашений о разграничении ответственности за обеспечение информационной безопасности внутри организации

б) Выработка специальных методик и политик, связанных с информационной безопасностью: анализ рисков, классификация систем и информации по уровням безопасности;

в) Поддержание в организации «атмосферы» информационной безопасности, в частности, регулярное информирование персонала по этим вопросам;

г) Обеспечение обязательности учета вопросов информационной безопасности при стратегическом и оперативном планировании;

д) Обеспечение обратной связи (оценка адекватности принимаемых мер безопасности в существующих системах) и координация внедрения средств обеспечения информационной безопасности в новые системы или сервисы;

е) Анализ инцидентов в области информационной безопасности, выработка рекомендаций;

Распределение ответственности за обеспечение безопасности

а) Определение ресурсов, имеющих отношение к информационной безопасности, по каждой системе;

б) Для каждого ресурса (или процесса) должен быть назначен ответственный сотрудник из числа руководителей. Разграничение ответственности должно быть закреплено документально;

в) Для каждого ресурса должен быть определен и закреплен документально список прав доступа (матрица доступа)

Процесс внедрения новой информационной системы

а) 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.

б) Все внедряемые компоненты должны быть проверены на совместимость с существующими частями системы.

Контрольные вопросы:

1. Процесс принятия новой информационной системы
2. Как распределять ответственность за обеспечение безопасности?
3. Зачем нужно создавать форумы по ИБ?

Лабораторная работа №3

Изучение классификации и управление ресурсами

по ограничению инцидентов ИБ

Цель работы – изучить классификации и управление ресурсами по ограничению инцидентов ИБ.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

Инвентаризация ресурсов

а) 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]

б) Программные ресурсы: приложения, операционные системы и системное программное обеспечение, средства разработки в) 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)

г) Вычислительные и коммуникационные сервисы, вспомогательные услуги: отопление, освещении и т.п.

Классификация ресурсов Все ресурсы должны быть классифицированы по степени важности.

Для каждого класса должны быть регламентированы следующие действия:

1. копирование
2. хранение
3. передача почтой, факсом, электронной почтой
4. передача голосом, включая мобильные телефоны, голосовую почту
5. уничтожение

Контрольные вопросы:

1. Инвентаризация ресурсов.
2. Классификация ресурсов.

Лабораторная работа №4

Обеспечение безопасности персонала

Цель работы – научиться обеспечивать безопасность персоналу.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

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 секьюрити инциденты и неисправности[1]

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 российской специфике это, в зависимости от последствий: дисциплинарные, административные или даже уголовные)

6. Регулярное обучение персонала по вопросам безопасности

Контрольные вопросы:

7. Безопасность при выборе персонала

8. Зачем нужна проверка персонала при приеме на работу?

9. Нужно ли реагировать на секьюрити инциденты и неисправности? Обоснуйте ответ.

Лабораторная работа №5

Обеспечение физической безопасность

Цель работы – научиться обеспечивать физическую безопасность.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

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

1. Документы на всех видах носителей и вычислительная техника, в случае если ими не пользуются, а также в нерабочее время, должны храниться в запираемом помещении

2. Ценная информация, когда она не используется, должна храниться в защищенном месте (огнеупорный сейф, выделенное помещение)

3. 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

4. Должны быть приняты надежные меры, исключающие несанкционированное использование копировальной техники в нерабочее время

5. Распечатки, содержащие ценную (конфиденциальную) информацию должны изыматься из печатающего устройства немедленно.

Контрольные вопросы:

1. Безопасность оборудования
2. Безопасность кабельной системы
3. Безопасное уничтожение оборудования при списывании
4. Безопасность рабочего места

Лабораторная работа №6

Управление коммуникациями и процессами

Цель работы – научиться обеспечивать безопасность персоналу.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

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

Служебные инструкции и ответственность.

Контроль изменений в операционной среде

• Идентификация и запись важных изменений

• Оценка потенциального последствий таких изменений

• Формальное утверждение процедуры внесения изменений

• Взаимодействие со всеми заинтересованными лицами при внесении изменений

• Процедуры определения ответственности и возврата в исходное состояние при неудачных попытках изменений

Служебные инструкции и ответственность. Процедуры реагирования в случае инцидентов (1)

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 (2)

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

Управление внутренними ресурсами. Запись действий операторов

Обязательной регистрации в системных журналах регистрации должны подвергаться:

• Время старта и остановки системы

• Системные ошибки и действия по их исправлению

• Подтверждение корректного обращения с входными и выходными данными

• Идентификатор оператора, совершившего действие, которое повлекло запись в журнал регистрации

Управление внутренними ресурсами. Ведение лога системных сбоев

• Анализ журнала системных сбоев на предмет корректности и завершенности процесса устранения последствий сбоев;

• Анализ произведенных действий на предмет соответствия установленным процедурам

Управление сетью

• Ответственность персонала за осуществление сетевых и локальных операций должна быть разделена;

• Должна быть определена ответственность и установлены процедуры управления удаленным оборудованием, включая оборудование в сегментах пользователей;

• При передаче информации через сети общего пользования должны применяться специальные средства обеспечения целостности и конфиденциальности. Для обеспечения работоспособности сетевых компьютеров должны быть разработаны специальные процедуры

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. Соглашения при передачи информации и ПО

• Назначение ответственных за процесс приема-передачи

• Определение процедур уведомления отправителя, получателя, и процедуры приема-отправки

• Минимальные технические стандарты для сообщений и для их передачи

• Идентификация способа доставки

• Ответственность за задержку и потерю данных

• Использование цифровой подписи объектов перед передачей критичной информации

• Стандартизация методов чтения и записи информации (данных и программного обеспечения) другие методы защиты критичных данных, такие как криптография и т.п.

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 при передаче информации и программного обеспечения. Безопасность электронной почты

При разработке политик необходимо учитывать следующие моменты:

1. Возможные атаки на электронную почту (например: вирусы, перехват, уничтожение, искажение)

2. Защита вложений

3. Порядок допуска персонала к использованию электронной почты

4. Определение ответственности сотрудников за нанесение вреда компании (компрометация имиджа, разглашение коммерческой тайны) в результате использования электронной почты;

5. Порядок использование криптографии для защиты электронных сообщений

6. Архивирование сообщений электронной почты, которые могут в последствии быть предъявлены в качестве доказательств в суде; 7. Регламентация

правил проверки сообщений, которые не могут быть однозначно аутентифицированы

Безопасность при передаче информации и программного обеспечения. Безопасность электронного офиса

1. Уязвимости информации в офисной системе, например, запись телефонных разговоров, конфиденциальность звонков, сохранение факсов, несанкционированный доступ к сообщениям электронной почты;

2. Политика и соответствующие инструкции по совместному использованию ресурсов (например, использование корпоративных электронных досок) 3.

Запрещение электронной обработки конфиденциальной информации, если система не обеспечивает должный уровень безопасности

4. Ограничение доступа к информации, связанной с выбором персонала (пример, персонал, работающий на засекреченные проекты)

5. Определение категорий персонала (постоянного и временного) и бизнес-партнеров, которым разрешен доступ в систему, а также определение разрешенных точек доступа

6. Ограничение выбранных ресурсов для специальных категорий пользователей

7. Идентификация статуса пользователей

8. Резервное копирование информации

9. Планы восстановления после аварийных ситуаций

Контрольные вопросы:

1. Что в себя включает управление коммуникациями и процессами?

Лабораторная работа №7

Исследование контроля доступа

Цель работы – исследовать контроль доступа.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

Политика контроля доступа

Политика должна учитывать следующее:

1. Требования по безопасности отдельных бизнес приложений

2. Идентификация всей информации, связанной с бизнес приложениями

3. Политика распространения и авторизации информации, например, необходимо знать принципы и уровни безопасности и иметь классификацию информации

4. Соответствие между контролем доступа и политикой классификации информации в разных системах и сетях

5. Значимые законы о защите информационных ресурсов

6. Стандартные профили доступа для всех типовых категорий пользователей

7. Управление правами пользователей в распределенных системах со всеми типами соединений

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 доступом пользователя.

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 доступом пользователя. 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.

Управление доступом пользователя. 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.

Ответственность пользователей.

Оборудование пользователей, оставляемое без присмотра

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.

Контроль доступа в операционную систему. Процедура входа в систему (log on) (1)

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.

Контроль доступа в операционную систему. Процедура входа в систему (log on) (2)

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.

Контроль доступа в операционную систему. 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.

Контроль и управление доступом к приложениям

Прикладная система должна:

- Управлять доступом пользователей к информации и системным вызовам приложений в соответствии с определенной политикой безопасности
- Обеспечивать защиту от несанкционированного доступа к системным утилитам
- Иметь возможность предоставлять доступ к информации только ее владельцу

Требования по ограничению доступа к информации

- Система меню для управления доступом к функциям прикладных программ
- Информация о функциях информационных систем и приложений должна предоставляться пользователю, в зависимости от уровня его доступа (необходима соответствующая редакция пользовательской документации и системного меню).
- Управление правами доступа пользователей (читать, писать, удалять, выполнять)
- Обеспечение отправления выходных данных приложений с важной информацией только на авторизованные терминалы, включая периодическую проверку выходных данных, чтобы убедиться, что избыточная информация там отсутствует.
- Изоляция особо важных систем

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. (1)

Требования безопасности:

1. Обеспечение физической защиты места удаленной работы, включая физическую безопасность здания или ближайшего окружения

2. 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

3. Учет возможной угрозы неавторизованного доступа к информации или ресурсам, от иных близких к удаленному пользователю людей, например, семья, друзья

Мобильные компьютеры и пользователи.

Удаленная работа. (2)

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

Контрольные вопросы:

1. Для чего нужен контроль 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

Разработка и техническая поддержка вычислительных систем

Цель работы – исследовать разработку и техническую поддержку вычислительных систем.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

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

Безопасность приложений. 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

Безопасность приложений. Проверки и средства управления(1)

1. Контроль сессий и автоматического выполнения заданий на предмет отклонений от обычного использования ресурсов.

2. Контроль изменений использования ресурсов по сравнению с предыдущими:

- запусками программ
- измененииями файла
- 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

Безопасность приложений. Проверка выходных данных(2)

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:

1. Управленческий подход к использованию СКЗИ внутри организации, включая основные принципы, какие именно классы информации должны быть защищены

2. Политика управления ключами, включая методы для восстановления зашифрованной информации в случае утери, компрометации или уничтожения ключей

3. Распределение обязанностей: кто и за что несет ответственность

4. Внедрение политики

5. Управление ключами

6. Порядок определения адекватного уровня криптографической защиты

7. Стандарты, которые могут быть внедрены и адаптированы в организации (какие решения подходят для каких бизнес процессов)

Криптографические средства управления.

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.

Контроль объектов операционной системы

1. Обновление библиотек должно выполняться только с разрешения руководства

2. Если возможно, ОС должна содержать только исполняемые файлы

3. 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)

4. После всех изменений в библиотеках должна быть обеспечена проверка всех регистрационных журналов

5. Предыдущие версии должны быть сохранены для непредвиденных случаев

Безопасность системных файлов.

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.

Безопасность системных файлов.

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

1. Документальное закрепление типовых уровней доступа

2. Обеспечение, того, что изменения сделаны авторизованными пользователями

3. Идентификация всего программного обеспечения, информации, баз данных, аппаратного обеспечения, которое требует изменений

4. Получение формального разрешения для детализации предложений до начала работ

5. Обеспечение того, что авторизованные пользователи принимают (проверяют) изменения до их внедрения

6. Обеспечение безопасного внедрения изменений без последствий для бизнеса

7. Обеспечение изменений системной документации после каждой модификации, а также архивация старой документации или ее отклонение

8. Обеспечение контроля версий для всех обновлений программного обеспечения

9. Обеспечение протоколирования всех запросов на изменение

10. Обеспечение соответствующих изменений оперативной и пользовательской документации

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

Безопасность процессов разработки и поддержки. 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

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?

Лабораторная работа №9

Управление непрерывностью бизнеса

Цель работы – исследовать управление непрерывностью бизнеса.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

Процесс управления непрерывным ведением бизнеса

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

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

1. Условия вступления в действие планов (как оценить ситуацию, кто в нее вовлечен)

2. Контр аварийные 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

3. 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

4. Процедуры восстановления, в которых описаны действия по возвращению к нормальному процессу бизнес операций

5. Разработка программы, в которой описаны, как и когда план будет протестирован и процесс внедрения этого плана

6. Действия по информированию и обучению, которые разрабатываются для понимания персоналом процесса обеспечения непрерывности бизнеса и гарантии, что этот процесс продолжает быть эффективным

7. 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) 6.

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

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

Соответствие системы основным требованиям

Цель работы – исследовать соответствие системы основным требованиям.

Формируемые компетенции или их части

Индекс	Формулировка:
ПСК-6.1	способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления
ПСК-6.2	способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления
ПСК-6.3	способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях
ПСК-6.4	способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления

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 дисциплинарные 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 компании Автоматизированная система компании создана для выполнения бизнес задач. Любое использование системы для решения задач отличных от основной цели недопустимо. В случае обнаружения системами слежения такого несоответствующего 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

Соответствие требованию законодательства. 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.

Контрольные вопросы:

1. Соответствие требованиям законодательства
2. Соответствие политике безопасности
3. Соответствие требованиям системного аудита

Список литературы:

1. Менеджмент инцидентов информационной безопасности : стандарт.

2. ISO 17799 : международный стандарт.