СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Основы управления информационной безопасностью***

Блок Б1, обязательная часть, Б1.О.23
цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2021 г.

Разработчик (составитель)
к. ф.-м. н., доцент
Гнатенко Ю. А.
ученая степень, должность, ФИО

Стерлитамак 2022

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3	4				5
			неуд.	удовл.	хорошо	отлично	
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.	Обучающийся должен: знать основные принципы политики управления доступом в компьютерных системах.	Отсутствие навыков	В целом успешное, но непоследовательное владение основными навыками составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем	В целом успешное, но содержащее отдельные пробелы владения навыками составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем	Успешное и последовательное владение основными навыками составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем	Практические работы №1-№5
	ОПК-1.2. Способен администрировать средства защиты	Обучающийся должен: уметь внедрять средства защиты	Отсутствие умений	В целом успешное, но не систематическое применение методологических	В целом успешное, но содержащее отдельные пробелы	Сформированное умение применять методологические принципы	Защита доклада, сообщения, реферата

	информации в компьютерных системах и сетях.	информации в компьютерных системах и сетях.		принципов внедрения средств защиты информации в компьютерных системах и сетях.	применения методологических принципов внедрения средств защиты информации в компьютерных системах и сетях.	внедрения средств защиты информации в компьютерных системах и сетях.	
	ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах.	Обучающийся должен: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационно	Отсутствие знаний	Неполные представления об основных принципах политики управления доступом в компьютерных система	Сформированные, но содержащие отдельные пробелы представления об основных принципах политики управления доступом в компьютерных система	Сформированные систематические представления об основных принципах политики управления доступом в компьютерных система	Тест

		й безопасности информационных систем					

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)

Критерии оценки тестов (в баллах)*:*

- *по 1 баллу выставляется студенту за каждый правильный ответ в задании теста;*
- *0 баллов выставляется студенту, если ответ на тест неправильный.*

Тест

Перечень заданий для оценки уровня сформированности компетенции ОПК-1 (индикатор достижения компетенции ОПК-1.1)

Низкий уровень

1.Выбирите функции управления
а) Планирование+
б) Организация+
в) Мотивация+
г) Развитие
д) Контроль+
2 Методы анализа конфликт логических данных:
статистический метод;+
математический метод;+
системно-экспертный метод;
исторический анализ;+
компаративный анализ.+
3 Выбрать стадии реализации системы управления информационной безопасностью:
а) формирование политики в области рисков.+
б) анализ бизнес-процессов.+
в) согласование рисков с экспертами
г) анализ рисков.+
д) формирование целевой концепции.+
4. Какие пункты включает «Замкнутый жизненный цикл системы управления информационной безопасностью»
а) Аудит СУИБ+
б) Корректировка мер по минимизации рисков ИБ+
в) планирование мер по минимизации рисков ИБ+
г) согласование запланированных мер
д) проверка +
5. СУИБ включает в себя:
а) организационную структуру,+
б) политики,+
в) распределение прав и обязанностей,
г) осуществление на практике,+
д) процессы и ресурсы+
8. Назовите методы управления информационной безопасности
а) административные+
б) инженерно-технические+
в) правовые+
г) теоретические+
д) экономические+
е) социально-педагогические
9. Типы мотивов в коллективе

а) мотив как внутренне осознанные потребности;+
б) мотив как внешняя осознанная потребность;
в) мотив как инструмент удовлетворения потребности +
г) мотив как намерение, побуждающее поведение; +
10. Мероприятия для обеспечения защиты информации в автоматизированной системе управления
а) формирование требований к защите информации в автоматизированной системе управления;+
б) разработка системы защиты автоматизированной системы управления;+
в) согласование системы защиты автоматизированной системы управления и ввод ее в действие;
г) обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления;+
д) обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления.+
11 Разработка системы защиты автоматизированной системы управления включает
а) проектирование системы защиты автоматизированной системы управления; +
б) согласование системы защиты автоматизированной системы управления
в) разработку эксплуатационной документации на систему защиты автоматизированной системы управления.+
12. Признаки конфликта
а) наличие ситуации, которая воспринимается участниками как конфликтная; +
б) неделимость объекта конфликта, т.е. объект конфликта не может быть поделено между участниками конфликтного взаимодействия; +
в) желание участников прекратить конфликтную взаимодействие для достижения своих целей.
13 Угрозы безопасности информации определяются на каждом из уровней автоматизированной системы управления по результатам:
а) оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей;+
б) анализа возможных уязвимостей автоматизированной системы управления;+
в) анализа возможных способов реализации угроз безопасности информации и последствий от нарушения как отдельных свойств безопасности информации, так и автоматизированной системы управления в целом;+
г) анализа текущей модели нарушителя ИБ.
14 Методы руководства коллективом
а) авторитарный+
б) либерально-попустительский+
в) демократический+
г) власть провокации
д) власть вознаграждения;+
е) власть эксперта+
15. Основные требования к системе защиты автоматизированной системы управления должны содержать:
а) класс защищенности автоматизированной системы управления; +
б) перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система управления; +
в) объекты защиты автоматизированной системы управления на каждом из ее уровней; +
г) требования к мерам защиты информации, применяемым в автоматизированной системе управления;

д) требования к защите информации при взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;
16. При проектировании системы защиты автоматизированной системы управления необходимо:
а) определять типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа); +
б) определять методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе управления; +
в) выбирать меры защиты информации, подлежащие реализации в рамках системы защиты автоматизированной системы управления; +
г) определять виды и типы средств защиты информации, обеспечивающие реализацию технических каналов утечки информации;
д) определять структуру системы защиты автоматизированной системы управления.
17. Внедрение системы защиты автоматизированной системы управления включает:
а) настройку программного обеспечения автоматизированной системы управления; +
б) согласование программного обеспечения автоматизированной системы управления с ФАПСИ;
б) разработку документов, определяющих правила и процедуры (политики), реализуемые оператором для обеспечения защиты информации в автоматизированной системе управления в ходе ее эксплуатации; +
в) внедрение организационных мер защиты информации; +
18Методы сбора конфликтологической информации
а) Наблюдение;+
б) изучение документов;+
в) опрос;+
г) метод case-study-probably;
д) экспертная оценка+
ожности реализации угроз безопасности информации в автоматизированной системе управления.

Средний уровень

1 «Управление информационной безопасностью» это _____ (Ответ циклический) процесс, включающий осознание _____ (Ответ степени необходимости) защиты информации и постановку задач; сбор и анализ данных о _____ (Ответ состоянии) информационной безопасности в организации; оценку информационных _____ (Ответ рисков); планирование мер по обработке рисков; _____ и _____ (Ответ реализацию и внедрение) соответствующих механизмов _____ (Ответ контроля), распределение ролей и ответственности,_____ и _____ (Ответ обучение и мотивацию) персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов _____ (Ответ контроля), оценку их эффективности и соответствующие корректирующие воздействия.
2 Основная цель СУИБ это _____ (Ответ защита) бизнес-процессов и _____ (Ответ знаний компании) от уничтожения или утечки
3 Оценка эффективности системы управления информационной безопасностью это _____ (Ответ системный процесс) получения и _____ (Ответ оценки объективных) данных о текущем состоянии систем, действиях и событиях происходящих в ней, устанавливающий уровень их соответствия определенным критериям
4 Рекомендации аудитора должны быть _____ и _____ (Ответ конкретными и

применимыми) к данной информационной системы, _____ (Ответ экономически) обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности.
5 Социальный конфликт это _____ или _____ (явное или скрытое) состояние противоборства объективно расходящихся интересов, _____ и _____ (Ответ целей и тенденций) развития социальных объектов,_____ и _____ (Ответ прямое и косвенное) столкновение социальных сил на почве противодействия существующему общественному порядку, особая форма исторического движения к новому социальному единству.
6 Систем управления информационной безопасность это часть системы _____ (Ответ менеджмента), основанная на анализе _____ (Ответ рисков) и предназначенная для _____,_____ (Ответ создания, внедрения) выполнения, мониторинга, пересмотра, поддержания и повышения уровня ИТ-безопасности.
7 Методы управления информационной безопасностью — это совокупность _____ и _____ (Ответ приемов и способов) воздействия на _____ (Ответ управляемый) объект для достижения поставленных целей.
8 «Управление информацией» в системе обработки информации – это функция _____ (ответ управления) получением, _____, (Ответ анализом,) сохранением, обновлением и распределением информации.
9 «Социально-психологические методы» это способы осуществления _____ (Ответ управленческих) воздействий на _____ (Ответ персонал), основанные на использовании закономерностей _____ и _____ (Ответ социологии и психологии).

Высокий уровень
1 Дайте развернутую характеристику руководителю среднего звена
2 раскройте разновидности подходов в управлении (не менее 3 разновидностей):
3 Процедуры выбора
4. Охарактеризуйте CRAMM
5. Охарактеризуйте методы мотивации как функцию управленческой деятельности

Перечень заданий для оценки уровня сформированности компетенции ОПК-1 (индикатор достижения компетенции ОПК-1.2)

Перечень типовых тем докладов, сообщений

Критерии оценки доклада, сообщения (в баллах)*:*

Шкала оценивания	Критерии оценивания
9-10	Доклад создан с использованием компьютерных технологий (презентация Power Point, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
6-8	Доклад создан с использованием компьютерных технологий (презентация Power

	Point, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
3-5	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
0-2	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

1 Принципы и условия отнесения информации к категории защищаемой;
2 Ресурсы предприятия, подлежащие защите с точки зрения ИБ;
3 Комплекс методов и средств защиты информации как объект управления ИБ;
4 Назначение и содержание политики ИБ предприятия;
5 Назначение и содержание структурных подразделений, частных политик безопасности. Средства их реализации;
6 Модель нарушителя политики безопасности;
7 Частная модель угроз информационной безопасности;
8 Типичные угрозы информации и уязвимости корпоративных информационных систем;
9 Содержание и организация процесса аудита ИБ;
10 Оценка рисков ИБ;
11 Отчетные документы по результатам аудита ИБ;
12 Выполнение рекомендаций по итогам проведения аудита ИБ;
13 Методология защиты информации как теоретический базис построения КСЗИ;
14 Принципы организации и этапы разработки комплексной системы защиты информации;
15 Принципы организации КСЗИ;
16 Основные требования, предъявляемые к КСЗИ;

Перечень тем рефератов

Критерии оценки реферата (в баллах)*:*

Шкала оцениван	Критерии оценивания

ия	
13-15	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы
9-12	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы
5-8	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод
0-4	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Реферат обучающимся не представлен

1 Основные положения теории управления в системах организационно-технологического типа.
2 Основы методологии принятия управленческого решения в системах организационно-технологического типа.
3 Требования, предъявляемые к комплексной системы защиты информации.
4 Основные этапы разработки комплексной системы защиты информации.
5 Факторы, влияющие на организацию комплексной системы защиты информации.
6 Порядок нормативного закрепления состава защищаемой информации.
7 Определение объектов защиты с точки зрения управления.
8 Источники и способы дестабилизирующего воздействия на информацию.
9 Каналы и методы несанкционированного доступа к информации.
10 Определение компонентов комплексной системы защиты информации.
11 Условия функционирования комплексной системы защиты информации.
12 Функциональная модель комплексной системы защиты информации.
13 Организационная модель комплексной системы защиты информации.
14 Информационная модель комплексной системы защиты информации.
15 Стадии создания комплексной системы защиты информации.
16 Структура и содержание документационного обеспечения стадий создания комплексной системы защиты информации.
17 Кадровое обеспечение функционирования комплексной системы защиты информации.
18 Нормативно-методическое и материально-техническое обеспечение комплексной системы защиты информации.

19 Общая технология управления комплексной системы защиты информации.
20 Принципы и методы планирования деятельности комплексной системы защиты информации.
21 Принципы и методы контроля функционирования комплексной системы защиты информации.
22 Управление комплексной системы защиты информации в условиях чрезвычайных ситуаций.
23 Общая характеристика подходов к оценке эффективности комплексной системы защиты информации.
24 Вероятностный подход к оценке эффективности комплексной системы защиты информации.
25 Статистические и экспертные методы оценки эффективности системы защиты информации.
26 Показатели защищенности комплексной системы защиты информации.
27 Организация обеспечения информационной безопасности автоматизированных систем
28 Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии.

Критерии оценки (в баллах)*:*

- 9-10 баллов выставляется студенту, если работа выполнена полностью, отчет содержит все необходимые пояснения к выполненному заданию;

- 6-8- балла выставляется студенту, если работа выполнена полностью, однако в отчете содержатся неполные пояснения к выполненному заданию;

- 1-5 баллов выставляется студенту, если задание выполнено, но отчет не сдан;

- 0 баллов, если работа полностью не выполнена.

Перечень заданий для оценки уровня сформированности компетенции ОПК-1 (индикатор достижения компетенции ОПК-1.3)

ПРАКТИЧЕСКАЯ РАБОТА №1: ПОНЯТИЙНЫЙ АППАРАТ НАПРАВЛЕНИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Цель: изучить понятийный аппарат направления «Информационная безопасность», получить опыт анализа и нормативных актов, формировать устойчивые навыки самостоятельной работы.

Методы и приемы: изучение теоретических источников, частичнопоисковая работа, анализ, формулирование понятий.

Ключевые слова: информационная безопасность, персональные данные, информационная система, информация, коммерческая тайна, государственная тайна, информационно-коммуникационные технологии, защита информации.

Порядок выполнения работы

1. Сопоставить предложенный перечень понятий с определениями, приведенными ниже.

2. Результат сопоставления оформить в виде пар чисел, где арабская цифра – ключевое понятие, а римская цифра – его определение

3. Составить отчет по практической работе.

Часть 1

1. Вирус (компьютерный, программный)

2. Информационная система общего пользования

3. Документированная информация

4. Аутентификация отправителя данных

5. Государственная тайна

6. Информационная система 7. Автоматизированная обработка персональных данных

8. Блокирование персональных данных

9. Автоматизированная система

10. Информация

11. Гриф секретности

12. Вредоносная программа

13. Доступ к информации

14. Информационно-телекоммуникационная сеть

15. Вспомогательные технические средства и системы

16. Защищаемая информация.

17. Безопасность персональных данных

I. программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

II. возможность получения информации и ее использования

III. технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

IV. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

V. реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него

VI. сведения (сообщения, данные) независимо от формы их представления

VII. временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)

VIII. зафиксированная на материальном носителе путем документирования с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

IX. подтверждение того, что отправитель полученных данных

соответствует заявленному

X. состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных

XI. технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных

XII. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно- розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

XIII. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

XIV. обработка персональных данных с помощью средстввычислительной техники

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

XVI. исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения

XVII. информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Часть 2

1. Ключ проверки электронной подписи
2. Межсетевой экран
3. Несанкционированный доступ
4. Коммерческая тайна
5. Информационные технологии
6. Идентификация
7. Источник безопасности персональных данных
8. Ключ электронной подписи
9. Конфиденциальность
10. Информационная система персональных данных
11. Контролируемая зона
12. Корпоративная информационная система
13. Накопитель информации
14. Контрагент
15. Нарушитель безопасности персональных данных
16. Конрагент
17. Недекларированные возможности

I. уникальная последовательность символов, предназначенная для создания электронной подписи

II. устройство, предназначенное для записи и (или) чтения информации на носитель информации. Устройство конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначено для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные

III. информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц

IV. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке (в том числе техническими средствами) в информационных системах персональных данных

V. функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

VI. процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов

VII. присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

VIII. уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи)

IX. обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

X. обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания

XI. совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

XII. пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание сторонних лиц, а также транспортных, технических и иных материальных средств

XIII. субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации

XIV. сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию

XV. доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных

XVI. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

XVII. локальное (однокомпонентное) или функционально-распределенное программное(программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Часть 3

1. Распространение информации
2. Побочные электромагнитные излучения и наводки
3. Правила разграничения доступа
4. Оператор
5. Пользователь ИСПДн
6. Обезличивание персональных данных
7. Предоставление информации
8. Оператор
9. Перехват информации
10. Обладатель информации

11. Носитель информации
12. Технические средства ИСПДн
13. Оператор ИС
14. Программная закладка
15. Персональные данные
16. Программное (программно-математическое воздействие)
17. Ресурс информационной системы

I. действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

II. именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы

III. действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

IV. гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных

V. несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ

VI. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

VII. физический объект, предназначенный для хранения информации

VIII. электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания

IX. код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожать информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства

X. действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

XI. лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования

XII. неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов

XIII. государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

XIV. лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

XV. средства вычислительной техники, информационно вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие

технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации)

XVI. совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

XVII. действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Часть 4

1. Технический канал утечки информации
2. Целостность информации
3. Уполномоченное оператором лицо
4. Электронный документ
5. Электронное сообщение
6. Разглашение информации, составляющей коммерческую тайну
7. Сайт в сети Интернет
8. Уничтожение персональных данных
9. Утечка информации по техническим каналам
10. Субъект доступа
11. Электронная подпись
12. Средства вычислительной техники
13. Система защиты персональных данных
14. Трансграничная передача персональных данных
15. Удостоверяющий центр
16. Угрозы безопасности персональных данных.

I. совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных

II. неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

III. действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору

IV. комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПДн

V. информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

VI. действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

VII. информация, переданная или полученная пользователем информационно-телекоммуникационной сети

VIII. способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения)

IX. лицо или процесс, действия которого регламентируются правилами разграничения доступа

X. документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

XI. передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

XII. совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети"Интернет"

XIII. юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом

XIV. лицо, которому на основании договора оператор поручает обработку персональных данных

XV. совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем

XVI. совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Содержание отчета: Тема, цель, ответы по тематическим частям в виде пар чисел, где арабская цифра – ключевое понятие, а римская цифра – его определение.

Информационные источники

1. Гафарова, Е.А. Организационно-правовое обеспечение информационной безопасности : учебное пособие / Е.А. Гафарова. - Челябинск : Издательство ЗАО «Библиотека А. Миллера». - 153 с. URL:http://elib.cspu.ru/xmlui/handle/123456789/7131 (дата обращения: 21.06.2021). – Библиогр. в кн. - ISBN 978-5-93162-170-8. – Текст: электронный.

2. http://www.e-nigma.ru/articles/

3. http://fstec.ru/

ПРАКТИЧЕСКАЯ РАБОТА № 2 ПРАВОВЫЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

Цель: научиться применять правовые акты в реальных ситуациях при организации защиты информации в учреждениях и на предприятиях, получить опыт разрешения правовых споров в области информационной безопасности, формировать законопослушность.

Методы и приемы: анализ, решение задач, проблемное обучение, мозговой штурм, семинар, кейс-метод.

Ключевые слова: государственная тайна, коммерческая тайна, персональные данные, защита информации, авторское право, интеллектуальная собственность, охранный документ, программа ЭВМ, база данных.

Порядок выполнения работы

1. Прочитать задачу, найти правовое обоснование и разрешить противоречивую правовую ситуацию.

2. Обсудить найденное решение, обосновать свою позицию аргументами и положениям правовых актов.

3. Решить задачи для самостоятельной работы по индивидуальному заданию

Раздел 1: Государственная тайна.

Задача 1. Гражданин Иванов, служил в качестве члена научно-исследовательской группы института "Прогресс". Иванов дал интервью для журнала «Метрополитен», в котором оценил радиационную обстановку в регионе с целью продемонстрировать суть его технической разработки по определению интенсивности излучения. Интервью с Ивановым была опубликована и стала общедоступной, и научным руководством Института "Прогресс". Администрация института подала заявление на Иванова о возбуждении уголовного дела по признакам преступлений, предусмотренных ст. 147 и ст. 183 Уголовного кодекса. Защитнику Иванова стало известно, что Иванов воспользовался для разработки своего технического устройства сведениями, составляющими коммерческую тайну. Будет ли Иванов привлечен к уголовной ответственности? Как ему избежать уголовной ответственности?

Задача 2. Репортер взял интервью у высокопоставленного чиновника Министерства экономического развития. В интервью были указаны сведения о стратегических запасах золота, платины и серебра. В отношении репортера и чиновника было возбуждено уголовное дело за распространение информации, составляющих государственную тайну. Что нужно предпринять журналисту и чиновнику, чтобы избежать уголовной ответственности по ст. 283 УК РФ?

Задача 3 Инженер Михайлов, который был гражданином Российской Федерации и инженер Скрипко, который был гражданином Украины, провели совместной научно-исследовательской работу, разработали новую технологию по виртуализации доменов. Оба соавтора имели доступ к сведениям, 107 составляющим государственную тайну. При рассмотрении заявки федеральным органом исполнительной власти по интеллектуальной собственности было установлено, что в новой технологии использованы сведения, составляющие государственную тайну. Какой орган имеет право рассматривать заявки на секретные изобретения, если они относится к техническим средствам в области разведывательной деятельности? Может ли в Российской Федерации быть выдан патент на секретное изобретение?

Задача 4 Химический комбинат г. Дубоссарск осуществил сброс производственных отходов в реку. Городские власти, получив от санэпидемслужбы города соответствующую информацию, не оповестили граждан об опасности. В результате купающиеся в реке получили ожоги. Имеется ли вина городской администрации? Приведите правовые нормы, обосновывающие вашу позицию.

Задача 5 Российский научно-исследовательский институт «Квант» являлся разработчиком и создателем информационной базы данных об испытаниях авиационно-космической техники. Институт получил разрешение Правительства РФ и соответственно своего министерства о направлении соответствующей информации о характеристиках авиационной аппаратуры в аналогичную научную организацию, находящуюся на территории Белоруссии. Однако представитель ФАПСИ, через которого предполагалось обеспечить передачу этой информации, обратил внимание дирекции института на конфиденциальный характер передаваемых сведений и, ссылаясь на этот факт, отказал НИИ в выделении каналов и средств для передачи информации. 108 Институт «Квант» обжаловал решение представителя ФАПСИ в Правительство РФ. Оцените ситуацию с точки зрения действующего законодательства.

Раздел 2: Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна

Задача 6 Общественная организация «За здоровье нации» обратилась к администрации Аргаяшской птицефабрики с заявлением о предоставлении информации о технике безопасности на предприятии: уровне ПДК в воздухе производственных помещений, уровне травматизма на производстве и выплате компенсаций по здоровьесбережению. Руководство предприятия отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются конфиденциальной информацией. Дайте разъяснения по существу сложившейся ситуации, приведите правовые нормы в обоснование своих доводов.

Задача 7 Сотрудники частной нотариальной конторы «Дело» на одном из своих совещаний приняли решение — создать собственный тайный архив, в котором собирать наиболее интересную частную информацию о всех своих клиентах и по мере необходимости использовать ее в своей повседневной деятельности. На следующий день был назначен руководитель архива и два эксперта и они начали собирать через своих коллег нужные сведения и данные о клиентах. Однако о факте создания тайного архива в нотариальной конторе «Дело» стало известно одному из клиентов, и он пожаловался на нотариусов в прокуратуру. Нарушила ли в этом случае контора законодательство?

Задача 8 Используя электронную сеть «Межсвязь», главный специалист коммерческого банка «Кубыш» Кусочкин в течение двух недель передавал с магнитных носителей информацию в департамент ценных бумаг ЦБ РФ. При этом он однажды рассказал о содержании направленных в ЦБ сообщений своему другу – юристу Министерства связи Савенко. Савенко, зная, что его товарищи из адвокатской фирмы «Прокруст» готовят иск против «Кубыш», немедленно переправил им полученную информацию. Адвокаты по достоинству оценили полученные сведения, использовали их при подготовке иска и в итоге – выиграли дело у банка. Узнав об этом, председатель правления коммерческого банка «Кубыш» Кубышкин уволил Кусочкина с работы за разглашение коммерческой тайны. Кусочкин не согласился с решением Кубышкина и обжаловал его действия в суде. Проанализируйте ситуацию с точки зрения норм информационного права и квалифицируйте действия Кусочкина, Савенко и Кубышкина.

Задача 9 Журналисты провели расследование совместно с общественной организацией «Маяк» и выявили повышенный уровень радиоизлучения в деревне Дербишево, находящейся на расстоянии 60 км от химкобината «Маяк». Об этом было рассказано в газете «За правое дело». Имеются ли в действиях журналистов признаки злоупотребления правом? Оцените эту ситуацию с точки зрения

законодательства о средствах массовой информации. Какие меры здесь необходимо принять к нарушителям?

Раздел 3: Интеллектуальная собственность. Авторское право.

Задача 10 Лех Я.В. обратился в суд с иском к ООО «Гранада» о взыскании компенсации за нарушение исключительного права на произведение, компенсации морального вреда, возложении обязанности по удалению произведения с сайта. В обоснование иска указал, что общество разместило на своем сайте литературно-художественный публицистический очерк (документальный рассказ), посвященный дню защиты Земли, автором которого он является Лех. Разрешение на публикацию очерка на сайте ответчика он не давал. Путем размещения на сайте указанного очерка было нарушено его авторское неимущественное право. Представитель ответчика факт размещения произведения истца на сайте не отрицала, исковые требования признала в части компенсации за нарушение ответчиком авторского права истца, при этом ссылалась на завышенный размер компенсации, заявленный истцом. В части компенсации морального вреда иск не признала, ссылаясь на то, что неимущественные права истца ответчиком не нарушены. Отмечает, что «незаконно использованный» ответчиком очерк по количеству строк более чем в два раза превышает написанный им рассказ, авторские права на который были приобретены московским продюсером за 1000 долларов. При этом над очерком он работал около 4 месяцев, а рассказ написан за 1 день. Как разрешитъ этот спор с позиции норм информационного права?

Задача 11 Смирнов П.Б. обратился в суд с иском к Новиковой Е.О. о защите авторских прав. Свои требования истец мотивирует тем, что на странице 111 интернет-сайта ответчика неправомерно использована фотография, автором которой является истец, без его согласия на воспроизведение и доведение до всеобщего сведения, без заключения с истцом авторского лицензионного договора, без указания и ссылок на источник и автора произведения, что является нарушением ст. 1229, 1265, 1270, 1300 Гражданского кодекса Российской Федерации (далее по тексту ГК РФ). Ответчиком допущено искажение фотографии в частности: кадрирование, обрезка изображения, наложение на фотографию надписи изменение цветового фона изображения. Истец просил взыскать с Новиковой Е.О. денежную компенсацию за нарушение авторских исключительных прав на фотографию (произведение), компенсацию морального вреда за использование фотографии без указания авторства, судебные расходы по обеспечению доказательств нотариусом и расходы по оплате услуг представителя. Ответчик вину в неправомерном размещении в сети Интернет фотографии не признала, пояснила, что фотографию удалила, ее размещение носило некоммерческий характер. Считает заявленные истцом суммы к взысканию завышенными. Оцените ситуацию с позиции правовых норм. Какое решение должен принять суд?

Задача 12 Организация «Новые технологии», занимающаяся формированием информационных ресурсов, начала разработку новой программы для государственных информационных систем. Для обеспечения защиты информационных ресурсов в этой системе был использован криптографический алгоритм «Криптт» компании «Джомолунгма» . Правомерно ли использование этого криптоалгоритма в разрабатываемой программе? Если да, то при каких условиях?

Задача 13 ООО «Холдинг-М» в лице Москвина осуществляло предоставление возмездных Интернет услуг с применением 2-х электронных

терминалов «Инфоинтсэйл», на жестких дисках которых установлены и использовались для работы терминала два экземпляра программы для ЭВМ «Microsoft Windows XP Professional», обладателем авторских и смежных прав на которую является «Корпорация Microsoft». Вышеуказанные экземпляры ЭВМ являются контрафактными по следующими признакам: отсутствуют документы, подтверждающие приобретение копии программы «Microsoft Windows XP Professional»; в корпусе системного блока не имеется сертификата подлинности программы (СОА) с наименованием и уникальным буквенно-цифровым ключом программного продукта; отсутствует соглашение с правообладателем об участии в программе корпоративного лицензирования, тем самым ООО «Холдинг-М» использовало с целью получения прибыли программу для ЭВМ «Microsoft Windows XP Professional». Представитель ООО «ХолдингМ» Москвин пояснял, что документов, подтверждающих приобретение обществом операционной «Windows XP» у него не имеется. Оцените ситуацию с точки зрения авторского права.

Раздел 4 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Задача 14 Оператор ПК Абдуллин, согласно своим должностным обязанностям, приеме электронных носителей с материалами обязан был проверять их на 113 наличие вирусов. Пытаясь завершить работу как можно скорее, Абдуллин проигнорировал проверку на антивирусном программном обеспечении. В результате попадания вируса в компьютерную систему был испорчен готовый к печати оригинал-макет выпуска газеты. Редакция понесла убытки, был нанесен репутационный вред изданию. Оцените действия Абдуллина с точки зрения действующего законодательства.

Задача 15 Разработчик программного обеспечения Стив несколько лет работал в акционерном обществе "Галатея". В трудовом договоре не было указано на явно имущественные права на созданные программы в процессе трудовой деятельности программиста. Во время работы Стив разработал эффективную систему автоматизации учета товаров на предприятии. Увидев, что его программа дает значительный экономический эффект, Стив потребовал от руководства доплату к ежемесячному окладу. Руководство рассмотрело вопрос по оплате и отказалось осуществлять доплату, вместо этого они приняли на работу еще одного программиста. Стив, в надежде, что он не сможет прийти к соглашению с компаниями, модифицировал свою программу, в результате чего она перестала функционировать. Оцените сложившуюся ситуацию с точки зрения действующего законодательства. Как квалифицировать действия Стива?

Задача 16 Программисту Иванову было поручено создать базу данных по финансовым и нематериальным активам предприятия. В целях быстрейшего Иванов, стремясь выполнить свою работу как можно быстрее, проигнорировал 114 требования антивирусной защиты. В результате база данных и программная оболочка были повреждены, предприятию пришлось закупать новое программное обеспечение. На программиста было наложено административное взыскание штраф, с чем он не согласился и обжаловал действия администрации Имеются ли здесь нарушения законодательства об информации, информатизации, защите информации и трудового права?

Раздел 5 Неправомерный доступ к информации. Задача 17 Адвокат Хорошавин, работая в юридической фирме «Лига А» в качестве помощника генерального директора, получил несанкционированный доступ к программам других людей и постоянно

использовал их. Более того, часть информации, полученной в базах данных, адвокат Хорошавин продал заинтересованным людям. В то же время, из-за несанкционированного проникновения помощника генерального директора в вышеупомянутые программы, в них начали появляться сбои, после чего владельцы источников информации, чтобы найти причину сбоя программного обеспечения провели экспертизу и установили причину сбоев. Владельцы программ и баз данных потребовали строгого наказания Хорошавина. Оцените сложившуюся ситуацию с точки зрения действующего законодательства.

Задача 18 Сельский почтальон по просьбе своей дочери подслушивал телефонные разговоры ее мужа. Он постоянно вскрывал письма и рассказывал об их содержании своей дочери, жалея ее, ведь она могла остаться одна и воспитывать двоих детей, если муж уйдет от нее к другой женщине. Имеются ли нарушения законодательства?

Задачи для самостоятельного решения

1. Сотрудник завода Чернов попросил у знакомого бухгалтера дистрибутив на установку программы 1С. В процессе развертывания дистрибутива, Черновым была допущена серьезная ошибка и дистрибутив оказался испорченным. Не мудрствуя лукаво, Чернов решил вернуть другой дистрибутив, взятый в коммерческой фирме у другого знакомого бухгалтера. Оцените действия Чернова.

2. Разработчик программного обеспечения Шариков использовал часть алгоритма своего знакомого Кошечкина, уехавшего некоторое время назад в Европу. Шариков зарегистрировал программу в установленном порядке и получил охранный документ. Кошечкин узнал о коммерческом использовании Шариковым программного продукта и подал на него в суд. Необходимо классифицировать действия Шарикова и Кошечкина. Будет ли удовлетворен иск?

3. Петровский получил на телефон сообщение, в котором был прислан единоразовый пароль для входа в личный кабинет банковских транзакций его подруги Ивановской. Однажды Ивановская просила его телефон для проведения транзакций и, по-видимому, «привязала» номер к личному профилю интернет-банка. Петровский помнил номер карты Ивановской и, воспользовавшись единоразовым паролем, перевел часть денежных средств с банковской карты Ивановской на свой расчетный счет. Оцените действия Петровского и Ивановской с точки зрения информационной безопасности и норм права.

4. Гавриков, обладая специальными познаниями в области работы с электронными вычислительными машинами (далее - ЭВМ) и компьютерными программами, используя принадлежащую ему ЭВМ, имеющую подключение к сети Интернет, приобрел путем копирования с сайта«Fishki» компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации. Впоследствии посредством принадлежащего ему компьютерного оборудования, а также находящихся в его пользовании хостинговых сервисов с доменными именами использовал указанные вредоносные компьютерные программы для заражения 50 ЭВМ пользователей сети Интернет и построения из них контролируемой сети. Построив контролируемую сеть, Гавриков без ведома и согласия пользователей скопировал хранящуюся в памяти зараженных ЭВМ компьютерную информацию, содержащую сведения о логинах и паролях авторизации пользователей на различных Интернет-ресурсах. Данную информацию Гавриков планировал использовать в личных целях. Оцените действия Гаврикова, приведите правовые нормы в обосновании своих доводов.

5. Анисимов работал и занимал различные должности в отделе технической поддержки UNIX Общества с ограниченной ответственностью (далее ООО) «Приват Трейд». С Анисимовым было заключено соглашение о конфиденциальности для работников ООО «Приват Трейд», согласно которого конфиденциальной информацией является техническая, технологическая, коммерческая (финансовая), организационная или иная используемая в коммерческой деятельности информация, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности неограниченному кругу третьих лиц, и к которой нет свободного доступа на законном основании. В период с 2015 по 2016 годы Анисимов, находясь на своем рабочем месте, используя средства авторизации (логин и пароль), предоставленные ООО «Приват Трейд», и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, скопировал на USB – носитель информацию из базы данных ООО «Приват Трэйд», а именно: не менее 40.000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты. После чего Анисимов передал вышеуказанную 117 информацию Мусалову, который не был осведомлен о том, что полученная им информация охраняется внутренними документами ООО «Приват Трэйд». Оцените действия Анисимова и Мусалова с правовых позиций действующего законодательства.

6. Закрытое акционерное общество «1С АКЦИОНЕРНОЕ ОБЩЕСТВО» (далее – ЗАО «1С») обратилось в Арбитражный суд Костромской области с иском к обществу с ограниченной ответственностью «Арктур» (далее – ООО «Арктур») о взыскании компенсации за незаконное использование результатов интеллектуальной деятельности в размере 90 000 руб. Исковые требования мотивированы тем, что в ходе обыска сотрудниками ОРЧ БЭП при УВД Костромской области были изъяты два системных блока и ноутбук, при осмотре выявлено, что на жестких дисках установлены компьютерные программы для ведения учета хозяйственной деятельности «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)» и «1С: Предприятие 7.7. ПРОФ Комплексная поставка», имеющие признаки контрафактности. Согласно заключению эксперта от 28.04.2008 на жестких дисках, представленных на экспертизу системных блоков обнаружена информационная база с учетными данными ООО «Арктур», созданная с использованием программы «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)». Запуск предположительно контрафактной программы «1С: Предприятие 7.7. Комплексная поставка (сетевая версия)» без аппаратного HASP-ключа защиты, вопреки штатного режима регламентируемого разработчиком был возможен вследствие модификации исполняемого файла. Оцените исход правого спора, приведите правовые нормы в подтверждение своей позиции.

7. Должностное лицо - индивидуальный предприниматель Сидорова не представила в установленный срок в государственный орган - Управление Федеральной службы государственной регистрации, кадастра и картографии сведения о состоянии использованных в процессе индивидуальной деятельности геодезических пунктов. Имеется ли в действиях Сидоровой правонарушение?

8. В адрес Общества с ограниченной ответственностью «Мираторг», для подтверждения финансово-хозяйственных взаимоотношений выставлено требование об истребовании документов (информации) при проведении мероприятий налогового контроля в отношении Говоровой Н.Н. Конкурсный управляющий Общества с ограниченной ответственностью «Мираторг» (далее также - Общество) Хацевич А.А.

сообщил, что требование не получал, несмотря на то, требование в адрес Общества было направлено заказным письмом по юридическому адресу организации и почтовому адресу организации и по адресу конкурсного управляющего. Истребуемые документы (информация) для проведения встречной проверки должны быть представлены в пятидневный срок со дня получения требования. Ходатайства о продлении срока предоставления документов (информации) в соответствии с п.5 ст.93.1 Налогового кодекса Российской Федерации в налоговый орган от обязанного представить соответствующие сведения лица не поступало. Имеется ли в действиях конкурсного управляющего правонарушение? Обоснуйте ответ правовыми нормами.

9. Заместителем генерального директора ОАО «УТК» по юридической и кадровой работе Громовой было направлено обращение в адрес министра строительства, жилищно-коммунального и дорожного хозяйства Республики Коми и Председателя Государственного Совета Республики Коми, содержащего, в числе прочего, информацию о проводимой работе по подготовке наградных листов для поощрения благодарностью Главы Республики Коми работников ОАО «УТК» - генерального директора Гаврилова и первого заместителя генерального директора - финансового директора Миронова. В соответствии с должностной инструкции Громова обязалась выполнять требования действующего законодательства РФ, приказов, инструкций, положений и иных нормативных актов по обеспечению сохранности конфиденциальной информации, не разглашать и не передавать конфиденциальные сведения, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных обязанностей (договорных) обязанностей. Администрация ОАО «УТК» наложила на Громову административное взыскание за разглашение персональных данных работников, на что Громова не согласилась и обратилась в суд с иском по трудовому спору. Оцените исход правого спора, приведите правовые нормы в подтверждение своей позиции.

10. Руководитель отдела технических разработок ФАПСИ Куликов дал интервью журналу "Горизонты", отметив положительный опыт организации деятельности ФАПСИ в современных условиях. Интервью получило широкий резонанс среди читателей журнала, и редакция журнала выплатила гонорар Куликову. Руководству ФАПСИ стало известно об интервью Куликова и ему был объявлен выговор за выступление без разрешения руководства. Куликов расценил данное наказание как нарушение ч.1 ст. 29 Конституции РФ. Как можно расценить спор с точки зрения действующего законодательства?

11. Программист Якупов и адвокат Гришин создали компьютерную программу, для экспертной оценки подлинности рукописных текстов. Якупов и Гришин подали заявку в патентное ведомство России на выдачу патента на полезную модель. Патентное ведомство отклонило их заявку, указав, что программы для компьютеров не признаются патентоспособными изобретениями. Разработчики не согласились с данным отказом и обратились в суд. Необходимо дать разрешение данной спорной ситуации.

12. На совещании юридических и физических лиц, работающих в области информатики и телекоммуникаций, заместитель руководителя Торгово-промышленной палаты Российской Федерации Кошель в резкой форме покритиковал те организации, которые копируют и используют программные и технические средства информатики без разрешения собственника и допускают иные нарушения этических норм. А буквально на следующий день это выступление Кошеля было без сокращений опубликовано в «Вестях» и 120 обиженные организации потребовали от руководителя Торгово-

промышленной палаты снятия с должности выступавшего за нарушение норм Национального кодекса деятельности в области информатики и телекоммуникаций. Необходимо определить, как должен быть разрешен этот спор.

13. На пленарном заседании торгово-промышленной палаты, посвященном взаимодействию в области развития сферы телекоммуникаций в регионе, вице-президент палаты Голенищев подверг резкой критике руководителей тех организаций, которые только «имитируют деятельность». Большой фрагмент стенограммы встречи был опубликован в областной газете. Обиженные руководители телекоммуникационных предприятий потребовали публикации опровержения в газете, а также снятия с должности вицепрезидента Голенищева за нарушение им норм «Положения об этике», принятом в Торгово-промышленной палате в качестве локального акта внутреннего распорядка. Вам нужно определить, как нужно решить спор.

14. Программист Войнович и его приятель техник-связист Саламатов обратились в Министерство связи с просьбой выделить им интернеткоммуникации для консалтинговой деятельности зарубежным партнерам. В удовлетворении заявления им было отказано. Войнович и Саламатов обратились за защитой прав предпринимателей в прокуратуру. Необходимо определить нарушен ли в этом случае порядок выделения ведомственных сетей связи юридическим и физическим лицам и как должен поступить прокурор города.

15. Гражданка Никанорова заподозрила своего мужа в измене и, установила специальную программу ему на телефон, пока он спал. Также она приобрела диктофонное устройство с дистанционным управлением, выполненное в виде дизайнерской зажигалки. Проанализировав детализацию звонков, полученную с помощью установленного программного обеспечения и диктофонные записи, гражданка Никанорова убедилась в правоте своих подозрений относительно неверности супруга, после чего подала на развод. Супруг гражданки Никаноровой написал заявление о преступлении, совершенной его женой. Признаки какого преступного деяния были описаны в заявлении супруга? Укажите правовые нормы.

16. Писательница Левит получила большой гонорар за изданные в Китае ее книги по личностному развитию. Гонорар был перечислен на ее индивидуальный расчетный счет в «Уралоптобанк». Левит планировала использовать большую часть этих денежных средств на содержание приюта для животных «Спаси меня» известного зоозащитника Даллакяна, поэтому не подала налоговую декларацию о доходах. Налоговая инспекция запросила сведения о доходах Левит в «Уралоптбанк», банк сначала ответил отказом, а потом все-таки предоставил эти сведения, на основании которых налоговый инспектор выставил Левит предписание в виде штрафа и пени за неуплаченный налог на доходы. Разгневанная писательница подала на суд и налоговую инспекцию в суд. Как вы думаете, какое решение примет суд? Обоснуйте правовыми нормами свою позицию.

17. Заядлый охотник Михайлов купил на рынке бинокль повышенной видимости для использования его на охоте. Его приятель Дремов увидев такой бинокль, попросил его на некоторое время у Михайлова с целью подглядывания за своей женой, которая в соседнем квартале работала няней у состоятельных бизнесменов. Оцените действия Михайлова и Дремова с точки зрения действующего законодательства.

18. Начальником управления образования городского округа города Котельнича Червяковой в адрес руководителей образовательных учреждений направлено письмо с требованием о предоставлении в управление образования городского округа города Котельнича сведений об оплате ими и их подчиненными транспортного, земельного налога, налога на имущество. Указанные сведения представлены руководителями образовательных учреждений в управление образования городского округа города

Котельнича и в последующем были переданы начальником управления образования городского округа города Котельнича Червяковой в администрацию города Котельнича. Должностными обязанностями Червяковой не предусмотрено осуществление сбора, хранения, использования и распространения персональных данных руководителей и работников образовательных учреждений г. Котельнича, не связанных с осуществлением ими трудовой деятельности в образовательных учреждениях. Оцените ситуацию с точки зрения действующего законодательства.

19. Сотрудник рекрутингового агентства Жорин проводил отбор претендентов на должность личного помощника руководителя крупного промышленного предприятия. За хорошее выполнение этой работы ему была обещана персональная выплата от руководителя. Требования к будущему личному помощнику были следующие: высшее образование, модельная внешность, разговорный английский, кроме того девушка не должна быть замужем. Желая получить обещанную выплату Жорин в свободное от работы время съездил по адресам потенциальных претенденток и узнал от соседей их семейный статус. Как вы думаете имеет ли место нарушение законодательства?

Информационные источники:

1. http://www.garant.ru
2. http://www.consultant.ru
3. https://rospravosudie.com

ПРАКТИЧЕСКАЯ РАБОТА №3: РЕАЛИЗАЦИЯ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ

Цель: ознакомиться с моделями управления доступом, научиться составлять матрицу доступа и иерархию ролей для учреждения профессионального учреждения для целей реализации политики безопасности, получить опыт принятия мотивированного решения.

Методы и приемы: изучение теоретических источников, контент-анализ сайтов образовательных учреждений, моделирование (политики безопасности), структурное программирование, кейс-метод.

Ключевые слова: политика безопасности, матрица доступа, ролевое управление доступом, мандатное управление доступом, объектноориентированный подход в ролевом управлении доступом, наследование ролей, инкапсуляция ролей

Краткие теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.

Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное (дискреционное, избирательное) управление доступом; мандатное (полномочное) управление доступом.

Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту.

На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту.

Матрица доступа является самым простым подходом к моделированию систем управления доступом. С ростом организации, увеличивается опасность хищения информации, в том числе сотрудниками, возрастают финансовые и репутационные риски, это приводит к ужесточению политик и систем контроля. Любые избыточные права доступа сотрудников ведут к увеличению риска утечки информации, в связи с чем, происходит ужесточение политики ИБ, так как увеличиваются риски утечки информации.

Избирательная политика безопасности широко применяется в автоматизированных системах коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) 68 управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя. Полномочное управление доступом подразумевает, что:

1) все субъекты и объекты системы однозначно идентифицированы;

2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности, поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в автоматизированной системе проводится анализ угроз и рисков для информации и информационного обмена и определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей. Фрагмент матрицы доступа представлен в таблице 3.

Таблица 3 Пример матрицы доступа

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет

Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования, так как число связей в них пропорционально произведению количества пользователей на количество объектов, и тогда в этом случае принимаются решения в объектно-ориентированном стиле, способные эту сложность понизить. Таким решением является **ролевое управление доступом**.

Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 6).Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число 70 администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно. Ролевое управление доступом оперирует следующими основными понятиями: **пользователь** (человек, интеллектуальный автономный агент и т.п.); **сеанс работы пользователя; роль** (обычно определяется в соответствии с организационной структурой); **объект** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД); **операция** (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными); **право доступа** (разрешение выполнять определенные операции над определенными объектами).

Рис. 6. Схема ролевого управления доступом

Ролям приписываются пользователи и права доступа, то есть реализуется отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса раб0оты пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть

несколько сеансов. Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1.

Очевидно, что **наследование ролей** соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов. Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить формирование **иерархии ролей**, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), до роли "руководитель".

При формировании иерархии ролей учитывается принципом **минимизации привилегий**, то есть каждой роли разрешено только то, что необходимо для выполнения служебных обязанностей.

Порядок выполнение работы:

1. Изучить теоретические сведения
2. Найти сайт образовательного учреждения
3. Смоделировать политику безопасности образовательного учреждения и составить матрицу доступа для образовательного учреждения.
4. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий.
5. Ответить на контрольные вопросы. Оформить отчет.

Контрольные вопросы

1. Что понимается под политикой безопасности?
2. В чем заключается модель дискреционной политики безопасности?
3. В чем заключается модель мандатной политики безопасности?
4. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
5. Как соотносятся матрица доступа и ролевой доступ?
6. В каких случаях целесообразно использовать ролевой доступ?
7. В чем состоит принцип минимизации привилегий?

Содержание отчета: Тема, цель, матрица доступа учреждения, ролевой доступ, ответы на контрольные вопросы.

Информационные источники: 1. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: http://citforum.ru/security/articles/galatenko/- (дата обращения - 01.03.2017)

2. https://www.anti-malware.ru/node/13626#part4

ПРАКТИЧЕСКАЯ РАБОТА № 4
ПРИМЕНЕНИЕ ИНВЕРСИОННОГО МЕТОДА ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.

Цель: ознакомиться с инверсионным анализом ТРИЗ (теории решения изобретательских задач), научиться использовать инверсионный анализ для решения задач информационной безопасности, мотивировать обучающихся к расширению методологических оснований для будущей профессиональной деятельности.

Методы и приемы: работа по алгоритму, анализ, синтез, инвертирование, мозговой штурм, самостоятельная работа, решение задач.

Порядок выполнения работы

1. Изучить теоретические сведения, при необходимости обратиться к интернет-источникам.

2. Изучить учебную задачу.

3. Применить инверсионный метод для самостоятельного решения задач информационной безопасности.

Краткие теоретические сведения.

Инверсионный метод (Диверсионный анализ) — это один из разделов ТРИЗ (теории решения изобретательских задач – основоположник Альтшуллер Г.С.), направленный на выявление и предотвращение вредных явлений в системах различного генезиса — технических, информационных, организационных.

Суть метода состоит в инвертировании проблемной ситуации при выявлении технических противоречий в системе, то есть в создании системной диверсии.

Метод позволяет выявить явные и скрытые причины возможных отказов, уязвимостей, рисков, иных вредных явлений в системе, тем самым появляется возможность спрогнозировать и предотвратить проявление проблем такого рода, предусмотрев соответствующие меры при разработке или модификации системы.

Таким образом, метод применяется:

• для поиска причин вредных явлений;

• для прогнозирования возможных вредных явлений.

Применительно к информационной системе, реализованной посредством информационно-коммуникационных технологий, задача состоит в ее «взломе» и несанкционированном доступе к информации.

Как правило, инверсионный метод реализуется через последовательные стадии:

1. Инвертирование задачи.

2. Формулирование «диверсионных гипотез».

3. Выявление «диверсионных ресурсов». 4. Тестирование «диверсионных гипотез».

В более сложных ситуациях может быть использован более широкий набор инструментов анализа.

Рассмотрим алгоритм решения учебной задачи с применением инверсионного метода и возможные схемы решений.

Учебная задача «Об электронной оболочке»: Необходимо определить перечень уязвимостей электронной оболочки личных профилей профессорско-преподавательского состава (далее - ППС) вуза, предложить меры по устранению потенциальных угроз.

Согласно ГОСТ Р 56545-2015 «уязвимость» – это недостаток (слабость) программного (программно-технического) средства или ИС в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Информационная система – это совокупность содержащейся в базах данных (далее по тексту – БД) информации и обеспечивающих ее обработку информационных технологий и технических средств.

Стадия 1: Инвертирование задачи. Переформулируем задачу в виде: «Как взломать электронную оболочку личных профилей ППС и получить доступ к конфиденциальной информации?»

Стадия 2: Формулирование диверсионных гипотез. В вузе принят негласный шаблон составления логина профиля из фамилии и инициалов имени и отчества преподавателя. Таким образом, логин можно составить, исходя из сведений о фамилии, имени и отчества, данные сведения являются открытыми и доступны на сайте университета.

После определения логина, остается подобрать пароль.

Несложно просто подсмотреть пароль, либо при выполнении каких-либо работ попросить интересующего нас преподавателя войти в его профиль, ссылаясь на неработающий свой или какие-то неполадки системы. Этот способ допустим, если «добытчик» пароля является сотрудником и в силу своего должностного положения может осуществить описанную последовательность действий.

Если такая мера неосуществима, пароль можно вычислить, пользуясь специальным программным обеспечением. При известном логине, вычислительных ресурсов только «взлома» пароля требуется немного.

Существует множество программ, две наиболее популярные - advnced archive Password Recovery и Visaul Zip Password Recovery Processor.

Кроме вышеперечисленных способов можно попытаться подобрать пароль с клавиатуры, используя известную информацию о человеке – день рождения, имя любимого питомца, и т.д. Таким образом, предложены три диверсионные гипотезы для решения данной задачи.

Стадия 3: выявление диверсионных ресурсов.

На этой стадии необходимо составить список ресурсов, которые способствуют реализации диверсионных гипотез. Перечень диверсионных ресурсов может быть таким:

- наличие шаблона составления логина;
- низкий уровень дисциплины ППС в области информационной безопасности;
- незнание и/или несоблюдение элементарных правил сохранения своих идентификаторов и аутентификаторов;
- малая обеспеченность компьютерной техникой рабочих мест ППС, когда за одним персональным компьютером закреплено несколько сотрудников.

Стадия 4: тестирование диверсионных гипотез - определение процедуры тестирования и проведение тестов.

Процедура тестирования состоит в экспериментальной проверке «взлома» электронной оболочки личных профилей ППС, то есть реализации выдвинутых гипотез на стадии 2.

Проверкой установлено, что логины были определены по шаблону «фамилия+инициалы». Среднее время определения логинов – 10 минут.

Подбор паролей с помощью программного обеспечения к трем профилям осуществлен в среднем в течение 30 минут, таким образом, тестирование подтвердило правоту диверсионных гипотез и наличие уязвимостей в описанной информационной системе.

При подведении итогов решения учебной задачи были предложены следующие способы усиления информационной защиты электронной оболочки:

- рекомендация замены логина и пароля пользователя после первого входа и активации профиля;
- разработка инструкции для сотрудников о необходимости сохранения аутентификаторов и идентификаторов;
- регулярный инструктаж сотрудников по соблюдению правил обеспечения информационной безопасности системы.

Задачи для самостоятельного решения.

a. **Задача «О защите интеллектуальной собственности свободными лицензиями».** Определить уязвимости для нарушения авторского права при распространении интеллектуальных продуктов в правовом поле свободных лицензий. Для определенности рассмотретьсемейства Common Public License, Cretive Commons Zero, Cretive Commons ttribution, GNU Generl Public License.

b. **Задача «О применении нейросетей для выявления террористических угроз».** В США потратили миллиарды долларов на разработку искусственного интеллекта, способного заменить человеческие ресурсы (проект ELINT- electronic intelligence) в разведке путем прослушивания и анализа разговоров по телефонам и анализа контента информационных ресурсов, используемых потенциальными террористами. Когда проект ELINT был готов, президент Джимми Картер отозвал всех американских агентов с Ближнего Востока. С тех пор Соединенные Штаты не задержали ни одного крупного террориста. С помощью инверсионного анализа определите причину неудач.

c. **Задача «О проведении банковских транзакций».** Платежи физических лиц в настоящее время все чаще производятся с помощью смартфонов через личный профиль интернет-банка. Подтверждение платежей физическим лицом происходит через одноразовые пароли, высылаемые на привязанный номер мобильного оператора смс-сообщением. Определить уязвимости данной системы, используя методы инверсионного анализа.

d. **Задача «Защиты персональных данных».** С помощью инверсионного анализа определить уязвимости автоматизированной информационной системы (АИС) обработки персональных данных учреждения профессионального образования. Исходные данные АИС определить самостоятельно, используя сайт образовательного учреждения.

e. **Задача «О системе «Платон».** Используя инверсионный анализ, определите уязвимости системы «Платон» взимания платы с большегрузных автомобилей. Предложите меры для эффективного функционирования данной системы.

f. **Задача «Сетевой город».** В настоящее время в общеобразовательных школах введена система «Сетевой город». Определить уязвимости и способы защиты данной учебной системы.

g. **Задача «О стратегической космической онлайн игре EVE Online».** Взлом профиля противника в названной командной он-лайн игре дает множество игровых преимуществ, от перераспределения ресурсов, в том числе и реальных денежных средств, до тактического преимущества на отдельном этапе этой массовой многопользовательской он-лайн игры. Определите уязвимости профиля, используя инверсионный анализ и знание особенностей семиуровневой модели OSI.

h. **Задача «О сопровождении в социальной сети ВКонтакте».** Исследователи неоднократно поднимали вопрос о потенциальной угрозе национальной безопасности России, реализованной в социальных сетях. Экстремистские группы социальных сетей представляют реальную угрозу национальной безопасности страны, вовлекая до миллиона молодых граждан России, пропагандируя идеи политического экстремизма, национального и гендерного превосходства и неравенства. Подобных групп в социальных

сетях немало и, если какие-то из них блокируются техническими службами по заявлениям неравнодушных пользователей, то на их месте появляется множество других с таким же опасным контентом. Используя инверсионный анализ, предложите меры по защите подрастающего поколения от негативного информационного воздействия экстремистских групп на примере социальной сети «ВКонтакте».

Информационные источники: 1. Абрамов О.Ю. Диверсионный анализ Технических Систем на переходном этапе развития - [Электронный ресурс] // URL: http://triz-summit.ru/file.php/id/f5015/nme/TRIZ- (дата обращения: 15.02.2017)

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

3. Буслов Д.И., Холкин И.Н. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SP Hn // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. URL: http://cyberlenink.ru/rticle/n/kk-ispolzuydiversionnyy-nliz-triz-nyti-kriticheskuyu-uyzvimost-grozyschuyubezopsnosti-sp-hn (дата обращения: 11.04.2017).

4. Вишнепольски С. Как выявлять причины вреда и устранять риски. Инверсионный метод риск-анализа. iBooks Edition. Mx EPublishing, 2013. 131 с.

ПРАКТИЧЕСКАЯ РАБОТА №5: ПОСТРОЕНИЕ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.

Цель: ознакомиться с содержанием и структурой частной модели угроз безопасности в информационной системе персональных данных (ИСПДн), получить опыт создания частной модели угроз безопасности для учреждения, имеющего информационную систему обработки персональных данных.

Методы и приемы: изучение теоретических источников, анализ, работа по шаблону, проектный кейс-метод, частично-поисковая работа, самостоятельная работа.

Ключевые слова: частная модель угроз, персональные данные, информационная система, модель нарушителя, угрозы утечки информации, технические каналы утечки информации, защищенность информационной системы, вероятность реализации угроз, корпоративная сеть, несанкционированный доступ.

Порядок выполнения работы

1. Изучить исходные условия существующей ИСПДн
2. Копировать шаблон частной модели угроз
3. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.
4. Защитить свой проект частной модели угроз ИСПДн.

Исходные условия ИСПДн «Кадры»

Организация: ЗАО «Солнышко».

Директор: Иванов Иван Иванович.

Заместитель директора: Петрова Тамара Васильевна.

Начальник отдела кадров: Южина Мария Ивановна.

Сотрудники отдела кадров: Сидорова Александра Павловна, Копылова Юлия Фёдоровна.

Состав ИСПДн:

1. Персональные данные сотрудников организации:

фамилия, имя, отчество
дата и место рождения
пол
сведения об образовании
сведения о предыдущем месте работы
семейное положение
адреса регистрации и фактического проживания
номера контактных телефонов
индивидуальный номер налогоплательщика
номер страхового свидетельства пенсионного страхования
номер полиса обязательного медицинского страхования
данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 777 субъектов персональных данных (сотрудников) в пределах Организации.

2. Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.

Топология: АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему – рис. 7).

Корпоративная сеть: Организации не имеет подключения к сетям связи общего пользования и сетям международного информационного обмена. В состав каждого АРМ входят два жёстких диска, на первом установлена операционная система, прикладное программное обеспечение и общедоступная справочная информация, на втором – информация, составляющая персональные данные сотрудников Организации.

Комплект АРМ №1-3: Системный блок № XXXXXXX01-03, Монитор Samsung N710 – серийный номер YYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03,

В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.

Комплект сервера: Системный блок № XXXXXXX04, Монитор Samsung N710 – серийный номер YYYYYYY04, клавиатура Genius серийный номер ZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.

Сервер и коммуникационное оборудование установлены в типовой стойке.

Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSSS.

3. Технология обработки персональных данных:

Обработка персональных данных сотрудников включает весь перечень действий.

К работе на АРМ допущены сотрудники отдела кадров и заместитель директора.

Полный доступ ко всей информации на АРМ и сервере имеют заместитель директора и начальник отдела кадров.

Сотрудники отдела кадров имеют полный доступ только к каталогу «Личные дела», размещённой на диске №2 своего АРМ, и только на чтение информации из каталога «Личные дела» на сервере.

Системный администратор сегмента сети не имеет доступа к информации, составляющей персональные данные. Имеет права на инсталляцию,

настройку программного обеспечения, программных (программно-аппаратных) средств защиты сервера и АРМ № 1-3. Режим работы - одновременный.

Расположение: Отдельный кабинет по адресу: РФ, г. Отрадный, ул. Веселая,, дом 6, офис 25.

Помещение офиса оборудовано охранной сигнализацией и в нерабочее время сдается под охрану.

Доступ в помещение ограничен распорядительными актами Организации и автоматизированной системой контроля и управления доступа.

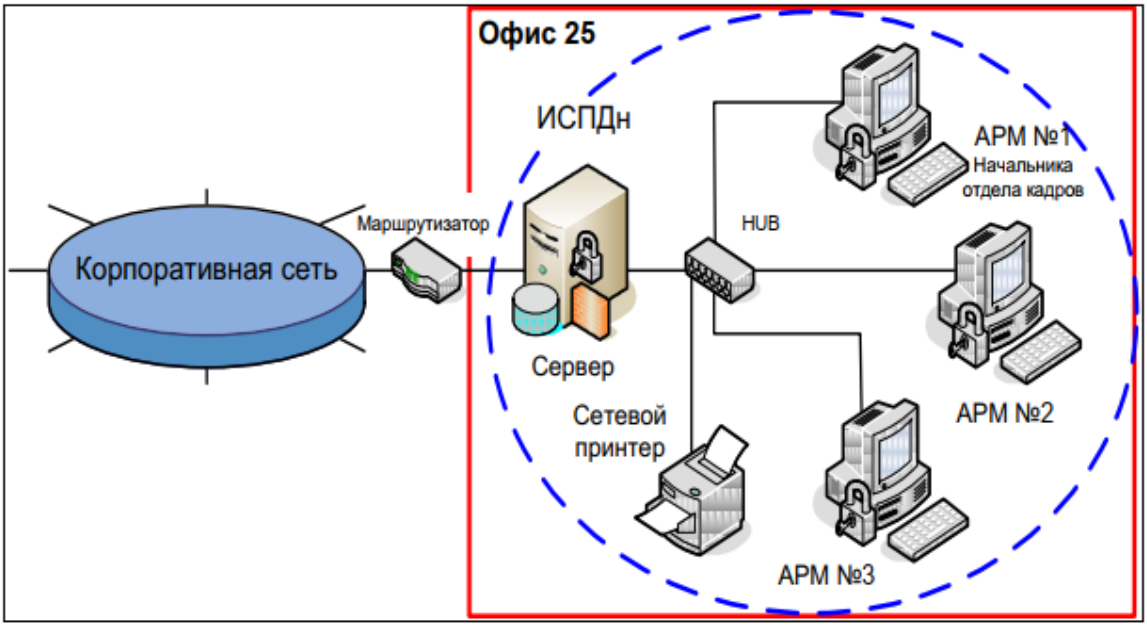

Рис. 7. Схема корпоративной сети

УТВЕРЖДАЮ

_____

_____

(должность руководителя организации)

_____

_____

(подпись)

«_____» _____ 201 ____г.

Частная модель угроз

безопасности персональных данных

при их обработке в ИСПДн

_____

(наименование ИСПДн)

СОГЛАСОВАНО

_____

_____

«_____» _____

201____ г

СОГЛАСОВАНО

_____

_____

«_____» _____

201____ г.

Сокращения, условные обозначения

Термины и определения

Введение.

Современная система обеспечения информационной безопасности должна строиться на основе комплексирования разнообразных мер защиты и должна опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации.

Результаты моделирования предназначены для выбора адекватных оптимальных методов парирования угроз.

На стадии моделирования проведено изучение и анализ существующей обстановки и выявлены актуальные угрозы безопасности ПДн в составе ИСПДн

Модель угроз построена в соответствии с

1. Описание ИСПДн

1.1. Описание условий создания и использования ПДн

1.2. Описание форм представления ПДн

1.3. Описание структуры ИСПДн

1.4. Описание характеристик безопасности

2. Описание подхода к моделированию угроз безопасности ПДн.

Модель угроз безопасности ПДн в составе ИСПДн разработана на основе методических документов ФСТЭК:

На основе «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн» проведена классификация угроз безопасности ПДн в составе ИСПДн и составлен перечень угроз безопасности ПДн в составе ИСПДн.

На основе составленного перечня угроз безопасности ПДн в составе ИСПДн с помощью «Методики определения актуальных угроз безопасности ПДн при их обработке в ИСПДн» построена модель угроз безопасности ПДн в составе ИСПДн и выявлены актуальные угрозы.

3. Классификация угроз безопасности персональных данных в ИСПДн

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угроз.

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, можно отнести:

_____

_____

_____

ИСПДн представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности.

Основными элементами ИСПДн являются:

Основными элементами канала реализации УБПДи являются:

Носители ПДи могут содержать информацию, представленную в следующих видах:

В целях формирования систематизированного перечня УБПДи при их обработке в ИСПДи угрозы классифицируются в соответствии со следующими признаками:

Реализация одной из УБПДи перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов ПДи:

Угрозы утечки ПДи по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и

приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДи и описываются следующим образом:

Угрозы, связанные с НСД, представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДи, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

3.1. Общее описание угроз безопасности ПДи, обрабатываемых в ИСПДи

При обработке ПДи в ИСПДи возможна реализация следующих видов УБПДи:

3.2. Угрозы утечки информации по техническим каналам.

Основными элементами угроз утечки информации по техническим каналам являются:

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

Возникновение угроз утечки акустической (речевой) информации, содержащаяся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

3.3. Угрозы несанкционированного доступа.

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в

том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

4. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн.

При обработке ПДн в ИСПДн, возможна реализация следующих видов УБПДн:

4.1. Угрозы утечки информации по техническим каналам.

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

4.1.1. Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового

ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Утечка акустической (речевой) информации может быть осуществлена:

_____

_____

_____

В ИСПДн не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн не предусмотрены.

Рассмотрение угроз утечки акустической (речевой) информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.2. Угрозы утечки видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:

_____

_____

_____

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от

них, соответственно отсутствует возможность непосредственного наблюдения посторонними лицами ПДн.

Рассмотрение угроз утечки видовой информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.3. Угрозы утечки информации по каналам ПЭМИН.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН в ИСПДн, избыточно, так как носители ПДн (технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин) находятся в пределах контролируемой зоны. Утечка ПДн по каналам ПЭМИН – маловероятна из-за несоответствия стоимости средств съема информации и полученной в результате регистрации ПЭМИН информации, а защита ПДн от данного вида угроз – экономически нецелесообразна.

4.2. Угрозы НСД к ПДн, обрабатываемым в ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы

непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в ИСПДн могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн возможны:

_____

_____

_____

5. Общая характеристика источников угроз НСД.

Источниками угроз НСД в ИСПДн могут быть:

_____

_____

_____

_____

_____

Нарушители:

_____

_____

_____

_____

_____

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн (Таблица 4)

Таблица 4 Категории нарушителей

Категория нарушителя	Способ доступа и полномочия

Носитель вредоносной программы.

Носителем вредоносной программыможет быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

_____

_____

_____

_____

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

1. пакеты передаваемых по компьютерной сети сообщений;
2. файлы (текстовые, графические, исполняемые и т.д.).

Аппаратная закладка.

В ИСПДи имеется опасность применения аппаратных средств, предназначенных для регистрации вводимой с клавиатуры информации, например:

В ИСПДи отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность установки аппаратных закладок посторонними лицами.

Существование данного источника угроз маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

5.1. Общая характеристика уязвимостей ИСПДи.

Уязвимость ИСПДи – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причины возникновения уязвимостей:

К основным группам уязвимостей ИСПДи, относятся:

Характеристика уязвимостей системного ПО.

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Характеристика уязвимостей прикладного ПО.

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – это

Специальные прикладные программы – это

Уязвимости прикладного программного обеспечения могут представлять собой:

5.3. Характеристика угроз непосредственного доступа в операционную среду ИСПДн.

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн:

Угрозы, реализуемые в ходе загрузки операционной системы

Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем

Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.Большая часть таких угроз – это угрозы внедрения вредоносных программ.

5.4. Общая характеристика УБПДи, реализуемых с использованием протоколов межсетевого взаимодействии.

Классификация угроз, реализуемых по сети, приведена в Таблице 5. В ее основу положено семь первичных признаков классификации.

Таблица 5 Описание угроз

№ п/п	Признак классификации	Тип угрозы	Описание

С учетом проведенной классификации можно выделить _____угроз, реализуемых с использованием протоколов межсетевого взаимодействия:

Анализ сетевого трафика.

Сканирование сети.

Угроза выявления пароля.

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Навязывание ложного маршрута сети.

Внедрение ложного объекта сети.

Отказ в обслуживании.

Удаленный запуск приложений.

5..5. Общая характеристика угроз программно-математических воздействий.

Программно-математическое воздействие- это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИС, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИС с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС.

Основными видами вредоносных программ являются:

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

5.6. Общая характеристика нетрадиционных информационных каналов.

Нетрадиционный информационный канал – это_____

Для формирования нетрадиционных каналов могут использоваться методы:

Методы компьютерной стеганографии предназначены для скрытия факта передачи сообщения путем встраивания скрываемой информации во внешние безобидные данные (текстовые, графические, аудио- или видеофайлы) и включают в себя две группы методов, основанных:

Нетрадиционные информационные каналы могут быть сформированы на различных уровнях функционирования ИСПДн:

5.7. Общая характеристика результатов несанкционированного или случайного доступа.

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

Нарушению конфиденциальности (копирование, неправомерное распространение), которое может быть осуществлено в случае утечки информации за счет:

Нарушению целостности (уничтожение, изменение) за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

Нарушению доступности (блокирование) путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

8. Определение уровня исходной защищенности ИСПДн

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

Таблица 6 Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению			
2. По наличию соединения с сетями общего пользования:			
3. По встроенным (легальным) операциям с записями баз персональных данных:			
4. По разграничению доступа к персональным данным:			
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
6. По уровню обобщения (обезличивания) персональных данных:			
7.По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			

В соответствии с Таблицей Описание угроз, _____ % характеристик ИСПДн соответствуют уровню не ниже "_____", следовательно, Y_1= _____ .

ИСПДн имеет _____ степень исходной защищенности.

9. Определение вероятности реализации угроз в ИСПДн

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вероятность (Y_2) определяется по 4 вербальным градациям этого показателя:

Таблица 7 Вероятность реализации угроз (вербальный показатель)

Градация	Описание	Вероятность (Y2)

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей приведена в следующей таблице

Таблица8 Вероятность реализации угроз (вероятностный показатель)

Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем категории Кп

По итогам оценки уровня исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (Таблица 9). Коэффициент реализуемости угрозы рассчитывается по формуле: $Y = (Y_1+Y_2)/20$.

Таблица 9 Коэффициент реализуемости угрозы

Угроза безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы

1.1. Оценка опасности угроз ИСПДн

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет 3 значения:

низкая опасность – ……;

средняя опасность – ……;

высокая опасность – ……..

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн являются:

_____

_____

_____

_____

Заключение

В настоящем документе проведена классификация УБПДн в ИСПДн, дано общее описание УБПДн и построена Модель угроз. В соответствии с требованиями методических документов ФСТЭК России, выявлены актуальные угрозы безопасности ПДн в ИСПДн, на основе которых в дальнейшем должны быть разработаны Требования по обеспечению безопасности ПДн в ИСПДн.

Построенная Модель угроз безопасности ПДн в ИСПДн применима к существующему состоянию ИСПДн при условии соблюдения основных (базовых) исходных данных:

- технические средства ИСПДн находятся в пределах контролируемой зоны;
- ИСПДн физически отделена от сетей общего пользования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях ИСПДн и др.

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности ПДн в ИСПДн должна быть подвергнута пересмотру.

Информационные источники:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

3. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России.

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Рейтинг-план дисциплины

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Правовое обеспечение информационной безопасности			0	50
Текущий контроль			0	50
Практическая работа №1	10	1	0	10
Практическая работа №2	10	1	0	10
Практическая работа №3	10	1	0	10
Практическая работа №4	10	1	0	10
Практическая работа №5	10	1	0	10
Рубежный контроль			0	50
Тест	1	25	0	25
Доклад	10	1	0	10
Реферат	15	1	0	15
итого			0	100
Поощрительные баллы				10
1. Активная работа на аудиторных занятиях	-	-	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение лабораторных			0	-10

занятий				
Итоговый контроль				
Зачет				
Итого			0	110

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = k × Максимальный балл,

где k = 0,2 при уровне освоения «неудовлетворительно», k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов БашГУ:
На зачете выставляется оценка:
• зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
• не зачтено - при накоплении от 0 до 59 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.