ДОГОВОР № -ДО-АИВ/2024
на оказание образовательных услуг

г. Москва « » 2024 г.

( ), именуемое в дальнейшем **Заказчик**, в лице , действующего на основании , с одной стороны, и

Общество с ограниченной ответственностью «Академия ИнфоВотч» (ООО «АИВ»), осуществляющее образовательную деятельность на основании лицензии от 20 апреля 2023г. № Л035-01298-77/00648477, выданной Департаментом образования и науки города Москвы, именуемое в дальнейшем «**Исполнитель**» и/или «**ООО «АИВ»**, в лице Генерального директора Харитонова Сергея Владимировича, действующего на основании Устава, с другой стороны, совместно именуемые Стороны, заключили настоящий Договор на оказание образовательных услуг (далее – «Договор») о нижеследующем:

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Дистанционные образовательные технологии** – образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся (слушателей) и педагогических работников.

1.2. **УПД** – универсальный передаточный документ, формируемый Исполнителем по форме, рекомендованной ФНС России, действующей на дату составления.

1.3. **Услуги** – заочные с применением дистанционных образовательных технологий образовательные услуги по обучению в рамках дополнительной образовательной программы повышения квалификации «Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур)», оказываемые Исполнителем Заказчику согласно условиям Договора, учебного плана, Программы (Приложение № 3 к Договору) и иных локальных актов Исполнителя.

2. ПРЕДМЕТ ДОГОВОРА

2.1. Исполнитель обязуется оказать, а Заказчик обязуется оплатить Услуги согласно условиям Договора и направить на обучение лиц, указанных в Приложении № 1 к Договору (далее – «Слушатели»).

2.2. Форма обучения: заочная с применением дистанционных образовательных технологий.

2.3. К освоению Программы допускаются лица, имеющие или получающие высшее или среднее профессиональное образование.

2.4. Срок освоения Программы на момент подписания Договора составляет 62 академических часа.

2.5. Сроки оказания Услуг: с _____ по _____.

2.6. Сроки оказания Услуг могут быть изменены:

2.6.1. По инициативе Исполнителя путем направления письменного уведомления о продлении срока, указанного в п. 2.5. Договора, на электронный адрес Заказчика и соответствующего Слушателя. В этом случае продление срока оказания Услуг осуществляется ввиду объективных причин (включая, но не ограничиваясь, отсутствием свободных временных слотов для итоговой аттестации в соответствии с указанной выше Дополнительной профессиональной программой; техническими работами на платформе системы дистанционного обучения и других причин). Исполнитель оставляет за собой право продлить срок, указанный в п. 2.5. Договора, что автоматически продлевает срок оказания Услуг на время задержки.

2.6.2. Изменение срока оказания Услуг может быть согласовано Сторонами при наличии уважительных причин не более 1 раза на 14 дней путем заключения дополнительного соглашения к Договору.

2.7. Одновременно с активацией доступа Слушателя в его личный кабинет, созданный посредством регистрации на платформе дистанционного обучения на сайте

https://lms.infowatch.ru (далее – «Личный кабинет») Слушателю открывается доступ к материалам Программы, а также на его электронную почту, указанную при регистрации, направляется ссылка на материалы Программы. Заказчик обязан обеспечить регистрацию Слушателей посредством входа в Личный кабинет.

2.8. После освоения Слушателями Программы и успешного прохождения промежуточной и итоговой аттестации им выдается удостоверение о повышении квалификации на бумажном носителе, а также оно дополнительно направляется на электронный адрес соответствующего Слушателя, указанный в Приложении № 1 к Договору, в виде ссылки для скачивания удостоверения в электронной форме. Удостоверение о повышении квалификации является документом о квалификации, подтверждающим ее повышение, согласно п. 10 ст. 60 Федерального закона от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации".

2.9. На электронный адрес соответствующего Слушателя, указанный в Приложении № 1 к Договору, дополнительно направляется электронный сертификат.

2.10. При освоении Программы параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение о повышении квалификации выдается одновременно с получением соответствующего документа об образовании и о квалификации.

2.11. Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также Слушателям, освоившим часть Программы и (или) отчисленным, выдается справка об обучении или о периоде обучения.

3. ПРАВА ИСПОЛНИТЕЛЯ И ЗАКАЗЧИКА

3.1. Исполнитель вправе:

3.1.1. Самостоятельно осуществлять образовательный процесс; Устанавливать системы оценок, формы, порядок и периодичность промежуточной аттестации Слушателей, применять к ним меры поощрения и меры дисциплинарного взыскания в соответствии с законодательством Российской Федерации, учредительными документами Исполнителя, Договором и локальными нормативными актами Исполнителя;

3.1.3. Привлекать для оказания услуг третьих лиц по своему усмотрению;

3.1.4. Не приступать к оказанию Услуг/приостановить оказание Услуг, предусмотренных Договором, в случае нарушения Заказчиком п. 5.2. Договора, в одностороннем порядке увеличить стоимость услуг в случае, предусмотренном п.3 ст. 54 ФЗ от 29.12.2012 № 273-ФЗ.

3.2. Слушателям предоставляются академические права в соответствии с частью 1 статьи 34 Федерального закона от 29 декабря 2012 г. № 273–ФЗ «Об образовании в Российской Федерации».

3.3. Заказчик вправе:

3.3.1. Получать информацию от Исполнителя по вопросам организации и обеспечения надлежащего предоставления Услуг.

3.3.2. Обращаться к Исполнителю по вопросам, касающимся образовательного процесса.

3.3.3. Пользоваться дополнительными образовательными услугами, предоставляемыми Исполнителем и не входящими в Программу на основании отдельно заключаемых договоров.

3.3.4. Получать информацию об оценке знаний, умений, навыков и компетенций Слушателей, а также о критериях этой оценки.

4. ОБЯЗАННОСТИ ИСПОЛНИТЕЛЯ И ЗАКАЗЧИКА

4.1. Исполнитель обязуется:

4.1.1. Зачислить Слушателей, выполнивших установленные законодательством Российской Федерации, учредительными документами, локальными нормативными актами Исполнителя условия приема, в качестве обучающихся (слушателей).

4.1.2. Предоставить Слушателям авторизированный доступ к системе дистанционного обучения на период обучения, а также осуществлять учебно-методическое руководство и обеспечение учебного процесса в дистанционной форме через компьютерную сеть Интернет и другие средства телекоммуникаций.

4.1.3. Организовать и обеспечить надлежащее предоставление Услуг. Услуги оказываются

в соответствии с учебным планом, в том числе индивидуальным (при его наличии), и расписанием занятий Исполнителя.

4.1.4. Обеспечить оказание Услуг в полном объеме в соответствии с Программой (частью Программы) и условиями Договора, условия их освоения.

4.1.5. Сохранить место за Слушателями в случае пропуска занятий по уважительным причинам (с учетом оплаты Услуг).

4.1.6. Обеспечить Слушателям уважение их человеческого достоинства, охрану жизни и здоровья, защиту от всех форм физического и психического насилия, оскорбления личности, охрану жизни и здоровья.

4.2. Заказчик обязуется:

4.2.1. Своевременно вносить плату за предоставляемые Услуги в размере и порядке, определенным Договором, а также по запросу Исполнителя предоставлять платежные документы, подтверждающие такую оплату.

4.2.2. Предоставить Исполнителю заявку установленной формы, документы и достоверную информацию в отношении Слушателей, требуемые для надлежащего исполнения Услуг по Договору.

4.2.3. Ознакомить Слушателей с лицензией Исполнителя на осуществление образовательной деятельности, Программой, иными локальными нормативными актами Исполнителя, касающимися организации и осуществления образовательной деятельности, правами и обязанностями обучающихся (слушателей), условиями Договора, а также ознакомить Слушателей с возможностью доступа к электронной информационно-образовательной среде Исполнителя без увеличения стоимости обучения.

4.2.4. Получить письменное согласие Слушателей на обработку их персональных данных с целью исполнения Договора и направить Исполнителю до начала оказания Услуг.

4.2.5. Для использования дистанционных образовательных технологий иметь материально-техническую базу согласно Приложению № 2 к Договору и обеспечить бесперебойную работу Интернет-канала, оборудования и программного обеспечения со своей стороны в течение срока оказания Услуг.

4.2.6. Обеспечить соблюдение Слушателями требований правил внутреннего распорядка, иных локальных нормативных актов Исполнителя, а также условий Договора.

4.2.7. Обеспечить использование учебно-методических материалов только для изучения Слушателями, указанными в Приложении № 1 к Договору, и не допустить использование учебно-методических материалов третьими лицами путем копирования, распространения, доведения до всеобщего сведения через сеть Интернет и иным образом. Запись, копирование, передача во временное пользование, несанкционированный прокат, публичный просмотр или распространение учебных пособий и услуг запрещается без специального письменного разрешения Исполнителя. В процессе оказания образовательных услуг запрещена аудиозапись и/или видеосъёмка без специального письменного разрешения Исполнителя. Любое из указанных действий является нарушением авторских, имущественных и иных прав Исполнителя и действующего законодательства в сфере интеллектуальной собственности, и может повлечь гражданскую, административную или уголовную ответственность. Нарушение условий настоящего пункта даёт Исполнителю право расторгнуть Договор полностью или частично в одностороннем внесудебном порядке, при этом Стороны обязуются осуществить приёмку фактически оказанных услуг и произвести взаиморасчёты исходя из фактически оказанного объёма услуг не позднее 10 рабочих дней с даты получения Заказчиком соответствующего уведомления от Исполнителя. Исполнитель оставляет за собой право прекратить оказание Услуг Слушателю, указавшему неверные реквизиты доступа к Программе, либо указавшему реквизиты доступа Слушателя, которому Услуги уже оказываются.

4.2.8. Выдать Слушателям переданные Исполнителем документы об образовании (ст. 2.6 и ст. 2.7. Договора).

4.2.9. В случае причинения Слушателями ущерба имуществу Исполнителя по требованию Исполнителя возместить причинённый ущерб в полном объёме.

4.3. Исполнитель и Заказчик взаимно перед друг другом при исполнении Договора обязуются обеспечить безопасность персональных данных, полученных друг от друга, при их обработке с соблюдением всех требований законодательства РФ, в том числе требования статьи 19 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных».

4.4. Стороны обязаны незамедлительно сообщить друг другу о допущенных ими либо ставшим им известным фактах разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами.

5. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ

5.1. Общая стоимость Услуг за весь период обучения составляет рублей. НДС не облагается на основании пункта 2 статьи 346.11 НК РФ.

5.2. Оплата Услуг по Договору производится Заказчиком путем единовременной 100% предоплаты в течение 5 рабочих дней с даты заключения Договора на основании счета Исполнителя. Счет считается предоставленным Исполнителем Заказчику, если он направлен на следующий электронный адрес Заказчика, указанный в разделе 10 Договора.

5.3. Обязательства Заказчика по оплате считаются исполненными в момент зачисления денежных средств в размере, указанном в п. 5.1. Договора, на расчетный счет Исполнителя, за исключением случаев, согласованных Сторонами.

5.4. В случае нарушения Заказчиком срока оплаты Услуг, Исполнитель вправе применить предусмотренные Договором и законодательством РФ меры ответственности.

5.5. Все расчеты по Договору осуществляются в рублях РФ в безналичной форме. Датой исполнения обязательств по оплате Услуг считается дата поступления денежных средств на корреспондентский счет банка, обслуживающего расчетный счет Исполнителя.

5.6. Допускается внесение оплаты за Заказчика третьим лицом при условии указания в реквизитах платежа данных счета, выставленного Заказчику.

5.7. Исполнитель выставляет УПД и направляет его для подписания Заказчику в течение 5 рабочих дней с даты завершения оказания Услуг в отношении всех Слушателей.

5.8. Заказчик в течение 3 рабочих дней с даты получения УПД должен либо подписать УПД и вернуть один экземпляр Исполнителю, либо направить Исполнителю мотивированный отказ от принятия оказанных услуг по Договору. Претензии Заказчика не могут выходить за рамки содержания и объема Услуг, оговоренных в Договоре. Если по истечении указанного в настоящем пункте срока Заказчик не осуществил возврат УПД и не предоставил письменного мотивированного отказа с указанием допущенных Исполнителем нарушений, услуги по Договору считаются оказанными Исполнителем, а УПД подписанным Сторонами.

5.9. Стороны могут обменяться электронными копиями всех документов, перечисленных в настоящем разделе. При этом моментом получения подписанного документа считается момент его отправки по электронной почте, указанной в п. 10 Договора. Направление электронных документов не освобождает Стороны от обязанности обмена подписанными оригиналами всех документов, перечисленных в настоящем разделе.

6. ИЗМЕНЕНИЕ И РАСТОРЖЕНИЕ ДОГОВОРА

6.1. Договор прекращает свое действие по следующим основаниям:

6.1.1. после завершения обучения по Программе;

6.1.2. при исключении Слушателей по основаниям, предусмотренным локальными нормативными актами, действующим законодательством, Договором;

6.1.3. по соглашению Сторон;

6.1.4. по инициативе Заказчика в одностороннем внесудебном порядке при условии уведомления Исполнителя не позднее, чем за 1 месяц и при условии оплаты Исполнителю фактически понесенных им расходов, связанных с исполнением обязательств по Договору, до даты издания приказа об отчислении Слушателей;

6.1.5. по инициативе Исполнителя в одностороннем внесудебном порядке следующих случаях:

- применение к Слушателям отчисления как меры дисциплинарного взыскания;

- невыполнение Слушателями по Программе обязанностей по добросовестному освоению такой Программы и выполнению учебного плана;
- установление факта нарушения порядка приема на обучение в ООО «АИВ», повлекшего по вине Заказчика незаконное зачисление Слушателей (Слушателя);
- просрочка оплаты стоимости Услуг;
- невозможность надлежащего исполнения обязательств по оказанию Услуг вследствие действий (бездействия) Заказчика и/ или Слушателя.
- при грубом нарушении локальных актов Исполнителя, которые распространяются на Слушателей.

6.1.6. по иным основаниям, прямо вытекающим из условий Договора, локальных нормативных актов Исполнителя или норм законодательства РФ.

6.2. Заказчик вправе отказаться от Услуг и/или исполнения Договора при условии тридцатидневного предварительного уведомления Исполнителя. В случае отказа Заказчик обязан выплатить Исполнителю 25% от стоимости Услуг, установленной в п. 5.1. Договора, что рассматривается Сторонами как заранее согласованные убытки Исполнителя. Возмещение Заказчиком указанной суммы осуществляется или 1) оплатой Заказчиком счета Исполнителя (в случае, если до даты отказа денежные средства в счет оплаты Услуг не поступили на расчетный счет Исполнителя); 2) или посредством удержания Исполнителем 25% стоимости Услуг, указанной в п. 5.1. Договора, при возврате Заказчику перечисленных денежных средств после отказа от Договора.

6.3. В случае отказа Исполнителя от Услуг Исполнитель возвращает Заказчику денежные средства в размере, указанном в п. 5.1. Договора, в течение 30 календарных дней с даты получения Исполнителем оригинала счета Заказчика на возврат.

6.4. Прекращение Договора по любым основаниям влечет за собой отчисление Слушателей с соблюдением требований Договора, локальных нормативных актов Исполнителя и действующего законодательства РФ.

7. ОТВЕТСТВЕННОСТЬ СТОРОН, ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

7.1. За неисполнение или ненадлежащее исполнение обязательств Стороны несут ответственность, предусмотренную законодательством РФ.

7.2. Если Слушатели без уважительной причины не приступили к обучению в сроки оказания Услуг, предусмотренные Договором (либо освоили соответствующую Программу не в полном объеме), в случае, если это произошло не по вине Исполнителя, Услуги Исполнителя подлежат оплате в полном объеме.

7.3. Оплата телекоммуникационных услуг по подключению Слушателей к сети интернет осуществляется Заказчиком и/ или Слушателями самостоятельно, без участия Исполнителя.

7.4. При этом Исполнитель не несет ответственности за отсутствие возможности для проведения обучения, задержку и/или приостановку в оказании Услуг, если это вызвано нарушением работы ЭВМ Заказчика/Слушателя, отсутствием и/или прерыванием доступа к сети Интернет провайдера Заказчика/Слушателя, нарушением работы приложения «Ассистент», облачной платформы для работы приложения (веб-сервиса), а также за иное нарушение связи, возникшее не по вине Исполнителя.

7.5. В случае нарушения работы веб-сервиса и приложения, Исполнитель имеет право заменить платформу на альтернативную. В случае такой замены Исполнитель имеет право изменить даты и время оказания Услуг с уведомлением Заказчика без обязательства возмещения убытков Заказчику.

7.6. Совокупная ответственность Исполнителя по Договору, по любому иску или претензии в связи с или в отношении Договора или его исполнения ограничивается суммой платежа, уплаченного по Договору Заказчиком Исполнителю.

7.7. Все споры между Сторонами, возникающие при исполнении, изменении или расторжении Договора, подлежат разрешению в суде по месту нахождения Исполнителя.

8. СРОК ДЕЙСТВИЯ ДОГОВОРА

8.1. Настоящий Договор вступает в силу с момента его подписания Сторонами и действует до момента его прекращения в соответствии с разделом 6 Договора или нормами действующего законодательства.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. В рамках оказания Услуг Исполнитель оставляет за собой право осуществлять аудио и видеозапись итоговой аттестации Слушателей. Заказчик гарантирует, что получил от Слушателей письменные согласия на осуществление аудиозаписи и видеосъемки с их участием. Все претензии и требования, связанные с указанными аудиозаписью и видеосъемкой, Заказчик обязуется урегулировать самостоятельно и за свой счет. Исполнитель имеет право использовать материалы указанных аудиозаписи и видеосъемки исключительно в целях доказательств оказания Услуг.

9.2. Слушателям и/ или Заказчику запрещается осуществлять аудио и видеозапись оказания Услуг без специального письменного разрешения Исполнителя.

9.3. Заказчик согласен с тем (и получил на это согласие Слушателей), что Исполнитель будет иметь право в любое время и в любом объеме размещать рекламные объявления и другие материалы рекламного характера в личном кабинете специалиста Заказчика на сайте .

9.4. Заказчик согласен с тем, что Исполнитель имеет право размещения логотипа Заказчика на своем сайте в разделе «Некоторые клиенты InfoWatch Академии» (https://infowatch.academy).

9.5. Все уведомления могут отправляться заказной почтой, телеграфом, факсом, электронной почтой по адресам Сторон, указанных в разделе 10 Договора. В случае изменения почтового и/или электронного адреса и (или) других реквизитов соответствующая Сторона должна уведомить об этом другую Сторону в письменной форме.

9.6. Ни одна из Сторон не вправе передавать свои права и обязанности по Договору третьим лицам без письменного согласия другой Стороны.

9.7. Настоящий Договор составлен в двух экземплярах, по одному для каждой из Сторон. Все экземпляры имеют одинаковую юридическую силу. Изменения и дополнения Договора могут производиться только в письменной форме к Договору и подписываться Сторонами или их уполномоченными представителями.

9.8. Изменения Договора оформляются дополнительными соглашениями к Договору.

10. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

ЗАКАЗЧИК:	ИСПОЛНИТЕЛЬ:
	ООО «АИВ»
Юридический адрес:	Юридический адрес: 121357, г. Москва,
р/с	ул. Верейская, д. 29, стр. 134, 7 этаж,
в	пом. 33
к/с	р/с 40702810538000204388
БИК	ПАО СБЕРБАНК
ОГРН	к/с 30101810400000000225
ИНН	БИК 044525225
КПП	ОГРН 1187746950313
Email:	Код по ОКВЭД 85.41.9
	ИНН 9731016250
	КПП 773101001
	Email: info@infowatch.ru
	Генеральный директор
_____	_____ С.В. Харитонов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0238DBC800C9B04981437026D4A6E6EAF2
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 29.11.2023 до 28.02.2025

Приложение № 1
к Договору на оказание образовательных услуг № -ДО-АИВ/2024
от « » 2024 г.

СПИСОК СЛУШАТЕЛЕЙ
направляемых в ООО «АИВ» для обучения
по дополнительной образовательной программе повышения квалификации:
«Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур)»

В соответствии с п. 2.1. Договора Исполнитель обязуется предоставить, а Заказчик обязуется оплатить образовательную услугу по обучению в рамках дополнительной образовательной программы повышения квалификации «Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур)» в соответствии с учебным планом, в том числе индивидуальным, и Программой и иными локальными актами Исполнителя и направить на обучение следующих слушателей:

1.
ФИО:
СНИЛС:
Дата рождения:
Документ, удостоверяющий личность: серия номер , выдан , дата выдачи: , код подразделения: .
Адрес места жительства:
Номер телефона:
Адрес электронной почты:
Документ об образовании (серия, номер, дата выдачи, кем выдан, специальность (направление)):

2.
ФИО:
СНИЛС:
Дата рождения:
Документ, удостоверяющий личность: серия номер , выдан , дата выдачи: , код подразделения: .
Адрес места жительства:
Номер телефона:
Адрес электронной почты:
Документ об образовании (серия, номер, дата выдачи, кем выдан, специальность (направление)):

ЗАКАЗЧИК: **ИСПОЛНИТЕЛЬ:**
ООО «АИВ»

Генеральный директор

_____ _____ С.В. Харитонов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0238DBC800C9804961437026D4A6E6EAF2
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 29.11.2023 до 28.02.2025

Приложение № 2
к Договору на оказание образовательных услуг № -ДО-АИВ/2024
от « » 2024 г.

Технические требования
к оснащению учебного места Слушателя,
обучающегося с использованием дистанционных технологий

Требования к оборудованию Слушателя для оказания Услуг:

- персональный компьютер под управлением операционной системы Windows 10 и выше;
- видеокамера, микрофон и аудиосистема (колонки или наушники), подключенные к компьютеру;
- пакет MS Office 2016 и выше;
- выход в Интернет;
- Интернет браузер;
- возможность установки и использования приложения «Ассистент».

ЗАКАЗЧИК: **ИСПОЛНИТЕЛЬ:**
ООО «АИВ»

Генеральный директор

_____ _____ С.В. Харитонов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0238DBC800C9B04981437026D4A6E6EAF2
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 29.11.2023 до 28.02.2025

Приложение № 3
к Договору на оказание образовательных услуг № -ДО-АИВ/2024
от « » 2024 г.

ПРОГРАММА
заочных с применением дистанционных образовательных технологий образовательных услуг по обучению в рамках дополнительной образовательной программы повышения квалификации «Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур)»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая программа представляет собой совокупность требований, обязательных при реализации программы дополнительного профессионального образования повышения квалификации «Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур).», профстандарт утвержден приказом Министерства труда и социальной защиты Российской Федерации от «14» сентября 2022 г. № 525н **«Специалист по защите информации в автоматизированных системах»** (код В).

Программа разработана в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н, также на основании Приказа Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам" и на основании Федерального закона "Об образовании в Российской Федерации" от 29.12.2012 № 273-ФЗ.

Цели:

- формирование знаний и навыков по вопросам применения законодательства в сфере защиты информации от утечек, сбора и анализа требования к конфиденциальной информации, выявления потенциальных каналов утечки конфиденциальной информации и определения комплекса мер по предотвращению утечек
- практическая подготовка для выполнения работ по разработке и реализации Политик защиты данных в системах защиты от утечки данных (DLP системы), а также оценки эффективности применения соответствующих Правил.

Категория слушателей:

- инженер по защите информации
- специалист по защите информации I категории
- специалист по защите информации II категории
- специалист по защите информации

Организационно-педагогические условия

Образовательный процесс осуществляется на основании учебного плана и регламентируется расписанием занятий для каждого слушателя.

Срок обучения: 62/4/1 (ак. час, нед., мес.).

Режим занятий: 54 академических часа самостоятельного обучения, 6 академических часов практического занятия с использованием средств видеокоференц связи, 2 академических часа итоговой аттестации (зачета) с использованием средств видеокоференц связи.

Форма обучения: заочная с применением дистанционных образовательных технологий

Характеристика профессиональной деятельности слушателей

Область профессиональной деятельности слушателей:

- обеспечение защиты данных от утечек

Специалист по защите данных от утечек готовится к следующим видам деятельности: к участию в обеспечении безопасности информации с учетом требования эффективного функционирования автоматизированной системы, к участию в выявлении угроз безопасности информации в автоматизированных системах, к участию в принятии мер защиты информации при выявлении новых угроз безопасности информации в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дополнительной профессиональной образовательной программы

Специалист должен обладать общими компетенциями, включающими в себя способность:

- Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес.
- Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
- Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
- Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.

Специалист должен обладать профессиональными компетенциями, соответствующими основным видам профессиональной деятельности:

- Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы
- Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации
- Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы
- Выявление угроз безопасности информации в автоматизированных системах
- Принятие мер защиты информации при выявлении новых угроз безопасности информации
- Анализ недостатков в функционировании системы защиты информации автоматизированной системы
- Устранение недостатков в функционировании системы защиты информации автоматизированной системы

Требование к слушателям

Требования к образованию и обучению	Высшее образование - бакалавриат в области информационной безопасности

Для реализации программы задействован следующий кадровый потенциал:

- **Преподаватели учебных дисциплин** - обеспечивается необходимый уровень компетенции преподавательского состава, включающий высшее образование в области соответствующей дисциплины программы или высшее образование в иной области и стаж преподавания по изучаемой тематике не менее трех лет; использование при изучении дисциплин программы эффективных методик преподавания, предполагающих выполнение слушателями практических заданий.
- **Административный персонал** - обеспечивает условия для эффективной работы педагогического коллектива, осуществляет контроль и текущую организационную работу.
- **Информационно-технологический персонал** - обеспечивает функционирование информационной структуры (включая ремонт техники, оборудования, макетов иного технического обеспечения образовательного процесса).

Содержание программы повышения квалификации определяется учебным планом и календарным учебным графиком программы дисциплин (модулей), требованиями к итоговой аттестации и требованиями к уровню подготовки лиц, успешно освоивших программу.

Текущий контроль знаний проводится в форме наблюдения за работой обучающихся и контроля их активности на образовательной платформе, проверочного тестирования.

Промежуточный контроль знаний, полученных обучающимися посредством самостоятельного обучения (освоения части образовательной программы), проводится в виде тестирования.

Итоговая аттестация по Программе проводится в форме зачета и должна выявить теоретическую и практическую подготовку специалиста.

Слушатель допускается к итоговой аттестации после самостоятельного изучения дисциплин Программы в объеме, предусмотренном для обязательных внеаудиторных занятий и подтвердивший самостоятельное изучение сдачей поурочных тестов, а также лабораторного практикума.

Лица, освоившие Программу и успешно прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации.

Оценочными материалами по Программе являются блоки контрольных вопросов по дисциплинам, формируемые образовательной организацией и используемые при текущем контроле знаний (тестировании), лабораторный практикум, теоретические вопросы и практические задания для итоговой аттестации.

Методическими материалами к Программе являются нормативные правовые акты и техническая документация по изучаемым программным продуктам, положения которых изучаются при освоении дисциплин Программы. Перечень методических материалов приводится в рабочей программе образовательной организации.

УЧЕБНЫЙ ПЛАН
ПО ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

ЗАЩИТА ДАННЫХ ОТ УТЕЧЕК. ОТ АНАЛИЗА БИЗНЕС-ПРОЦЕССОВ ДО НАСТРОЙКИ И ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ (закрытый контур).
(профстандарт «Специалист по защите информации в автоматизированных системах» код B)

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоятельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттеста-ция	
1	Внедрение и техническая поддержка InfoWatch Traffic Monitor	30,0	9,5	15,3	5,2	
2	Обзор аналитических работ	6,5	2,5	3,0	1,0	
3	Правовые и организационные аспекты легитимизации DLP системы	3,8	1,3	2,0	0,5	
4	Настройка и использование программных средств InfoWatch	10,1	5,6	4,0	0,5	
5	Подготовка и реализация Концепции Политики защиты данных	9,6	0,4	3,2	6,0	
6	ИТОГОВАЯ АТТЕСТАЦИЯ	2,0			2,0	Зачет
	Всего:	62	19,3	27,5	15,2	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
ПО ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

ЗАЩИТА ДАННЫХ ОТ УТЕЧЕК. ОТ АНАЛИЗА БИЗНЕС-ПРОЦЕССОВ ДО НАСТРОЙКИ И ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ (закрытый контур).

(профстандарт «Специалист по защите информации в автоматизированных системах» код B)

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттеста-ция	

1	Внедрение и техническая поддержка InfoWatch Traffic Monitor	30,0	9,5	15,3	5,2	
1.1	Архитектура и технологии InfoWatch Traffic Monitor	4,4	1,6	2,8		
1.2	Тестирование	0,8			0,8	
1.3	Развертывание InfoWatch Traffic Monitor	2,9	0,9	2,0		
1.4	Тестирование	0,4			0,4	
1.5	Развертывание InfoWatch Device Monitor for Windows	2,5	1,0	1,5		
1.6	Тестирование	0,4			0,4	
1.7	Администрирование InfoWatch Traffic Monitor	3,7	1,2	2,5		
1.8	Тестирование	0,8			0,8	
1.9	Развертывание InfoWatch Device Monitor for Linux	1,7	0,7	1,0		
1.10	Тестирование	0,4			0,4	
1.11	Развертывание InfoWatch Vision	2,5	1,0	1,5		
1.12	Тестирование	0,4			0,4	
1.13	Развертывание InfoWatch Data Discovery	1,5	0,5	1,0		
1.14	Тестирование	0,4			0,4	
1.15	Развертывание InfoWatch Activity Monitor	3,5	2,0	1,5		
1.16	Тестирование	0,8			0,8	
1.17	Развертывание и настройка InfoWatch Prediction	2,1	0,6	1,5		
1.18	Тестирование	0,8			0,8	
2	Обзор аналитических работ	6,5	2,5	3,0	1,0	
2.1	Формирование плана аналитических работ и сбор требований	1,0	0,5	0,5		
2.2	Анализ данных в DLP системе	3,5	1,5	2,0		
2.3	Подготовка данных и формирование Концепции Политики защиты данных	1,0	0,5	0,5		
2.4	Тестирование	1,0			1,0	
3	Правовые и организационные аспекты легитимизации DLP системы	3,8	1,3	2,0	0,5	
3.1	Нормативное обеспечение использования DLP системы	1,7	0,7	1,0		
3.2	Организационное обеспечение	1,6	0,6	1,0		

	использования DLP системы					
3.3	Тестирование	0,5			0,5	
4	Настройка и использование программных средств Infowatch	10,1	5,6	4,0	0,5	
4.1	Настройка и использование Infowatch Traffic Monitor	5,8	3,3	2,5		
4.2	Настройка и использование Infowatch Device Monitor	3,8	2,3	1,5		
4.3	Тестирование	0,5			0,5	
5	Подготовка и реализация Концепции Политики защиты данных	9,6	0,4	3,2	6,0	
5.1	Подготовка Концепции Политики защиты данных	3,2	0,2	3		
5.2	Реализация Концепции Политики защиты данных	0,4	0,2	0,2		
5.3	Лабораторный практикум	6,0			6,0	
6	ИТОГОВАЯ АТТЕСТАЦИЯ	2,0			2,0	Зачет
	Всего:	62	19,3	27,5	15,2	-

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный график обучения является примерным, составляется и утверждается для каждого слушателя.

Срок освоения программы – 4 недели. Начало обучения – по мере набора слушателей. Примерный режим занятий: 0,5-3,0 академических часа в день (кроме практического занятия с использованием средств видеокоференц связи). Промежуточная и итоговые аттестации проводятся согласно графику.

№	Наименование модулей / дни	ВР	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	Внедрение и техническая поддержка InfoWatch Traffic Monitor	СР	2,0	3,0	3,0	3,0	3,0	3,0	3,0	3,0	3,0	2,0	2,0																			
2	Обзор аналитических работ	СР												2,0	2,0	2,0																
3	Правовые и организационные аспекты легитимизации DLP	СР															2,0	2,0														
4	Настройка и использование программных средств Infowatch	СР																	2,0	2,0	2,0	2,0	2,0									
5	Подготовка и реализация Концепции Политики защиты данных	СР																						0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	6,0
6	Итоговая аттестация																															2,0

Рабочая программа учебной дисциплины «Внедрение и техническая поддержка InfoWatch Traffic Monitor» (код В)

Цель: обеспечение глубоких знаний обучающихся в области использования, внедрения и администрирования средств защиты от утечки данных: IW Traffic Monitor, IW Device Monitor, IW Data Discovery и IW Vision в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс внедрения, администрирования и использования
средств защиты от утечки данных: InfoWatch Traffic Monitor, InfoWatch Device Monitor, InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Теоретические основы проектирования системы корпоративной защиты от внутренних угроз с использованием InfoWatch Traffic Monitor и его модулей
- Инструментарий, технологии, область их применения и ограничения при формировании корпоративной защиты от внутренних угроз информационной безопасности на основе InfoWatch Traffic Monitor и его модулей

Уметь:

- Проводить расследования инцидентов внутренней информационной безопасности с использованием InfoWatch Traffic Monitor и его модулей
- Администрировать InfoWatch Traffic Monitor и его модули
- Работать с консолью InfoWatch Traffic Monitor, InfoWatch Device Monitor for Windows
- Развертывать InfoWatch Traffic Monitor, InfoWatch Device Monitor, InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction
- Конфигурировать и обслуживать InfoWatch Traffic Monitor, InfoWatch Device Monitor, InfoWatch Data Discovery, InfoWatch Vision, InfoWatch Activity Monitor, InfoWatch Prediction

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 30,0 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 30,0 академических часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
	Внедрение и техническая поддержка InfoWatch Traffic Monitor	30,0	9,5	15,3	5,2	
1	Архитектура и технологии InfoWatch Traffic Monitor	4,4	1,6	2,8		
2	Тестирование	0,8			0,8	
3	Развертывание InfoWatch Traffic Monitor	2,9	0,9	2,0		
4	Тестирование	0,4			0,4	
5	Развертывание InfoWatch Device Monitor for Windows	2,5	1,0	1,5		
6	Тестирование	0,4			0,4	
7	Администрирование InfoWatch Traffic Monitor	3,7	1,2	2,5		
8	Тестирование	0,8			0,8	
9	Развертывание InfoWatch Device Monitor for Linux	1,7	0,7	1,0		
10	Тестирование	0,4			0,4	
11	Развертывание InfoWatch Vision	2,5	1,0	1,5		
12	Тестирование	0,4			0,4	
13	Развертывание InfoWatch Data Discovery	1,5	0,5	1,0		
14	Тестирование	0,4			0,4	
15	Развертывание InfoWatch Activity Monitor	3,5	2,0	1,5		
16	Тестирование	0,8			0,8	
17	Развертывание и настройка InfoWatch Prediction	2,1	0,6	1,5		
18	Тестирование	0,8			0,8	

Тема 1. Архитектура и технологии InfoWatch Traffic Monitor

- Назначение и состав Traffic Monitor
- Device Monitor: возможности и принципы работы
- Data Discovery: возможности и принципы работы
- Vision: возможности и принципы работы
- Режимы перехвата Traffic Monitor
- Архитектура системы Traffic Monitor
- Технологии анализа контента
- Создание политик защиты данных
- Мобильные устройства и удаленный доступ

Тема 2. Развертывание InfoWatch Traffic Monitor

- Подготовка к установке Traffic Monitor.
- Установка и настройка операционной системы Oracle Linux 7.9.
- Подготовка операционной системы РЕД ОС 7.3 для установки Traffic Monitor.
- Подготовка операционной системы Astra Linux 1.7.0 для установки Traffic Monitor.
- Поэтапная установка Traffic Monitor в текстовом режиме.
- Первоначальная настройка Traffic Monitor.
- Установка InfoWatch Data Analysis Service и его интеграция с Traffic Monitor.

Тема 3. Развертывание InfoWatch Device Monitor for Windows

- Аппаратные и программные требования для Device Monitor
- Поэтапная установка Device Monitor
- Настройка проверки сертификата сервера Traffic Monitor
- Интеграция Device Monitor со службами каталогов
- Установка агента на рабочую станцию
- Конфигурирование и обслуживание Device Monitor

Тема 4. Администрирование InfoWatch Traffic Monitor

- Диагностика работы
- Администрирование работы компонент
- Диагностика работы компонент
- Очистка места на сервере
- Администрирование очередей
- Настройка OCR экстрактора Google Tesseract
- Администрирование базы данных PostgreSQL

Тема 5. Развертывание InfoWatch Device Monitor for Linux

- Аппаратные и программные требования для Device Monitor for Linux.
- Подготовка к установке сервера Device Monitor for Linux.
- Поэтапная установка web консоли Device Monitor for Linux.
- Поэтапная установка сервера Device Monitor for Linux.
- Установка агента Device Monitor for Linux.

Тема 6. Развертывание InfoWatch Vision

- Аппаратные и программные требования Vision
- Подготовка к установке на Oracle Linux
- Поэтапная установка Vision
- Первоначальная настройка Vision
- Обслуживание сервера Vision

Тема 7. Развертывание InfoWatch Data Discovery

- Аппаратные и программные требования для Data Discovery.
- Настройка сетевых правил доступа.
- Поэтапная установка Data Discovery.
- Первоначальная настройка Data Discovery

Тема 8. Развертывание InfoWatch Activity Monitor

- Аппаратные и программные требования для Activity Monitor.
- Настройка сетевых правил доступа.
- Поэтапная установка Activity Monitor.
- Первоначальная настройка Activity Monitor.

Тема 9. Развертывание InfoWatch Prediction

- Аппаратные и программные требования для Prediction.
- Подготовка к установке на Oracle Linux.
- Поэтапная установка Prediction.
- Импорт конфигурации в Traffic Monitor.
- Первоначальная настройка Prediction.

Рабочая программа учебной дисциплины «Обзор аналитических работ» (код B)

Цель: обеспечение глубоких знаний обучающихся в области выявления информации, подлежащей защите, определения угроз, направленных на данную информацию и определения технологий, позволяющих предотвратить утечку информации в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить принципы выявления информации, подлежащей защите, технологии анализа контента, позволяющие предотвратить утечку информации, а также порядок формирования Политики защиты данных (как части Политики информационной безопасности) в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Методы сбора требований об информационных потоках организации
- Методы выявления информации, подлежащей защите
- Технологии анализа контента, реализованные в DLP системе InfoWatch Traffic Monitor
- Порядок подготовки Политики защиты данных

Уметь:

- Определять оптимальный метод сбора требований исходя из ситуации
- Комбинировать методы сбора требований с целью обеспечения полноты и оперативности получения информации
- Определять информацию, подлежащую защите, порядок хранения и передачи информации, подлежащей защите

- Определять угрозы защищаемой информации, а также технологии и способы предотвращения утечки защищаемой информации

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6,5 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 6,5 академических часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
	Обзор аналитических работ	6,5	2,5	3,0	1,0	
1	Формирование плана аналитических работ и сбор требований	1,0	0,5	0,5		
2	Анализ данных в DLP системе	3,5	1,5	2,0		
3	Подготовка данных и формирование Концепции Политики защиты данных	1,0	0,5	0,5		
4	Тестирование	1,0			1,0	

Тема 1. Формирование плана аналитических работ и сбор требований

- План аналитических работ
- Сбор требований
- Интервью
- Опросный лист
- Изучение документации
- Определение чувствительной информации

Тема 2. Анализ данных в DLP системе

- Технологии анализа контента
- Лингвистический анализ
- Текстовые объекты
- Эталонные документы
- Бланки
- Печати
- Выгрузки из баз данных
- Графические объекты
- Автолигвист

Тема 3. Подготовка данных и формирование Концепции Политики защиты данных

- Подготовка данных для формирования Концепции Политики защиты данных
- Формирование Концепции Политики защиты данных

Рабочая программа учебной дисциплины «Правовые и организационные аспекты легитимизации DLP системы» (код В)

Цель: обеспечение глубоких знаний обучающихся в области нормативно-правового и организационного обеспечения использования системы защиты данных от утечек (DLP системы) с учетом действующего Законодательства РФ и в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить законодательство РФ в сфере защиты информации, в том числе от утечек, организационное обеспечение, направленное на информирование сотрудников об использовании в организации системы защиты от утечки данных, а также порядок привлечения к ответственности сотрудников, в случае выявления фактов утечки с учетом действующего Законодательства РФ и в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

В результате обучения дисциплине слушатели должны:

Знать:

- Основные нормативные документы РФ в сфере защиты информации
- Порядок информирования сотрудников об использовании системы защиты от утечки данных
- Порядок привлечения сотрудников к ответственности в случае выявления фактов утечки данных

Уметь:

- Определять перечень и содержание локальных документов организации, направленных на защиту данных от утечек
- Определять порядок действий для обеспечения легитимности использования системы защиты данных от утечек
- Определять порядок действий по привлечению сотрудников к ответственности в случае выявления факта утечки защищаемой информации

Тема 1. Нормативное обеспечение использования DLP системы

- Конституция РФ
- Федеральный закон 149 – ФЗ
- Федеральный закон 152 – ФЗ
- Федеральный закон 98 – ФЗ
- Закон о государственной тайне
- Нормативные документы регуляторов
- Приказы ФСТЭК № 21 и №17

Тема 2. Организационное обеспечение использования DLP системы

- Личное и корпоративное
- Рекомендации к легитимизации DLP
- Нормативная документация
- Специально-технические средства
- Заключение по законодательству
- Примеры судебных решений
- Алгоритм увольнения сотрудника

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3,8 академических часа (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 3,8 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
	Правовые и организационные аспекты легитимизации DLP системы	3,8	1,3	2,0	0,5	
1	Нормативное обеспечение использования DLP системы	1,7	0,7	1,0		
2	Организационное обеспечение использования DLP системы	1,6	0,6	1,0		
3	Тестирование	0,5			0,5	

Рабочая программа учебной дисциплины «Настройка и использование программных средств Infowatch» (код B)

Цель: обеспечение глубоких знаний обучающихся в области администрирования программных продуктов АО «Инфовотч», позволяющих обеспечить защиту от утечки данных в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить возможности программных продуктов АО «Инфовотч» , позволяющих обеспечить защиту от утечки данных в соответствии с требованиями

профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дисциплины
В результате обучения дисциплине слушатели должны:
Знать:

- Интерфейс систем InfoWatch Traffic Monitor и InfoWatch Device Monitor.
- Порядок администрирования InfoWatch Traffic Monitor в части работы со списками и элементами управления системой.
- Порядок наполнения технологий, создания Объектов защиты и Политик защиты данных в InfoWatch Traffic Monitor.
- Порядок формирования сводных отчетов, поиска событий и визуализации информации о событиях в InfoWatch Traffic Monitor.
- Порядок администрирования InfoWatch Device Monitor в части работы со списками, настройками системы, группами компьютеров и пользователей.
- Порядок создания Политик и Правил в InfoWatch Device Monitor.

Уметь:

- Проводить подготовительные настройки и создавать Политики защиты данных в InfoWatch Traffic Monitor
- Формировать отчеты о событиях, зарегистрированных системой InfoWatch Traffic Monitor
- Выполнять действия по администрированию систем InfoWatch Traffic Monitor и InfoWatch Device Monitor

Структура и содержание дисциплины
Общая трудоемкость дисциплины составляет 10,1 академических часа (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 10,1 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
	Настройка и использование программных средств Infowatch	10,1	5,6	4,0	0,5	
1	Настройка и использование Infowatch Traffic Monitor	5,8	3,3	2,5		
2	Настройка и использование Infowatch Device Monitor	3,8	2,3	1,5		
3	Тестирование	0,5			0,5	

Тема 1. Настройка и использование Infowatch Traffic Monitor

- Вводная часть по настройке и администрированию ТМ

- Технологии "Категории и термины" и "Текстовые объекты"
- Технология "Эталонные документы"
- Технологии "Бланки" и "Печати"
- Технология "Выгрузки из БД"
- Технология "Графические объекты"
- Персоны
- Периметры
- Списки
- Объекты защиты данных
- Управление
- Политики
- Сводка
- События
- Отчеты

Тема 2. Настройка и использование Infowatch Device Monitor

- Вводная часть по DM
- Начало работы с Консолью управления DM
- Алгоритм подготовки к созданию политики в консоли DM
- Раздел Ресурсы
- Раздел Приложения
- Раздел Категории сигнатур
- Политики
- Правило для Application Monitor
- Правило для Clipboard Monitor
- Правило для Cloud Storage Monitor
- Правило для Device Monitor
- Правило для File Monitor
- Правило для FTP Monitor
- Правило для HTTP(S) Monitor
- Правило для IM Client Monitor
- Правило для Keyboard Monitor
- Правило для Mail Monitor
- Правило для Network Monitor
- Правило для Print Monitor
- Правило для ScreenShot Control Monitor
- Правило для ScreenShot Monitor
- Правило для File Operation Monitor
- Раздел Группы сотрудников и как на них назначить политику
- Раздел Группы компьютеров и как на них назначить политику
- Белые списки
- Настройки
- Установка агента

Рабочая программа учебной дисциплины «Подготовка и реализация Концепции Политики защиты данных» (код B)

Цель: обеспечение глубоких знаний обучающихся в области разработки и реализации Политики защиты данных, направленной на предотвращение утечки защищаемой информации в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям получить практические навыки разработки и реализации Политики защиты данных, направленной на предотвращение утечки защищаемой информации в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Порядок анализа предоставленных документов
- Порядок определения технологии анализа контента исходя из характера и требований к защищаемой информации
- Порядок определения объектов защиты исходя из выбранных технологий анализа контента, а также характера и требований к защищаемой информации
- Порядок определения доверенных отправителей и получателей защищаемой информации
- Порядок определения Политик защиты данных и правил реагирования системы

Уметь:

- Формировать Политику защиты данных
- Настраивать технологии анализа контента InfoWatch Traffic Monitor
- Создавать Объекты защиты
- Создавать Политики защиты данных InfoWatch Traffic Monitor
- Создавать Политики InfoWatch Device Monitor
- Оценивать результаты работы реализованных Политик и выполнять их доработку

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 9,6 академических часов (из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 3,6 академических часа, практическое занятие с использованием средств видеоконференц связи - 6 часов.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	

	Подготовка и реализация Концепции Политики защиты данных	9,6	0,4	3,2	6,0	
1	Подготовка Концепции Политики защиты данных	3,2	0,2	3		
2	Реализация Концепции Политики защиты данных	0,4	0,2	0,2		
3	Лабораторный практикум	6,0			6,0	

Тема 1. Подготовка Концепции Политики защиты данных

- Этапы подготовки Концепции
- Выявление требований и подготовка данных
- Формирование концепции

Тема 2. Реализация Концепции Политики защиты данных

- Используемые технологии анализа
- Объекты защиты
- Списки отправителей/получателей
- Политики защиты данных

ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Формы аттестации

Для проведения промежуточной и итоговой аттестации программы разработан фонд оценочных средств по программе, являющийся неотъемлемой частью учебно-методического комплекса.

Объектами оценивания выступают:

- степень освоения теоретических знаний;
- уровень овладения практическими умениями и навыками по всем видам учебной работы, активность на занятиях.

Текущий контроль знаний обучающихся проводится преподавателем, ведущим занятия в учебной группе, на протяжении всего обучения по программе.

Текущий контроль знаний включает в себя наблюдение преподавателя за учебной работой обучающихся и проверку качества знаний, умений и навыков, которыми они овладели на определенном этапе обучения посредством выполнения упражнений на практических занятиях и в иных формах, установленных преподавателем.

Промежуточная аттестация - оценка качества усвоения обучающимися содержания учебных блоков непосредственно по завершении их освоения, проводимая в форме зачета посредством тестирования.

Итоговая аттестация - процедура, проводимая с целью установления уровня знаний, обучающихся с учетом прогнозируемых результатов обучения и требований к результатам освоения образовательной программы. Итоговая аттестация обучающихся осуществляется в форме зачета.

Слушатель допускается к итоговой аттестации после изучения тем образовательной программы в объеме, предусмотренном для лекционных и практических занятий.

Лицам, освоившим образовательную программу повышения квалификации «Защита данных от утечек. От анализа бизнес-процессов до настройки и использования DLP-системы (закрытый контур)» по профстандарту «Специалист по защите информации в автоматизированных системах» (код В)» и успешно прошедшим итоговую аттестацию, выдается **удостоверение о повышении квалификации** установленного образца с указанием названия программы, календарного периода обучения, длительности обучения в академических часах.

Для аттестации обучающихся на соответствие их персональных достижений требованиям соответствующей ОП созданы фонды оценочных средств, включающие типовые задания, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций.

Фонды оценочных средств соответствуют целям и задачам программы подготовки специалиста, учебному плану и обеспечивают оценку качества общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся.

Критерии оценки обучающихся

Предмет оценивания (компетенции)	**Объект оценивания (навыки)**	**Показатель оценки (знания, умения)**
Специалист должен обладать общими компетенциями (ОК), включающими в себя способность: • Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес. • Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. • Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. • Осуществлять поиск и использование информации, необходимой для эффективного выполнения	**Специалист должен обладать профессиональными компетенциями (ПК), соответствующими основным видам профессиональной деятельности:** • Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы • Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации • Внесение изменений в эксплуатационную документацию и организационно-	**Знания:** • Принципы формирования политики информационной безопасности в автоматизированных системах • Программно-аппаратные средства защиты информации автоматизированных систем • Принципы организации и структура систем защиты программного обеспечения автоматизированных систем • Нормативные правовые акты в области защиты информации • Организационные меры по защите информации **Умения:** • Формировать политику безопасности программных компонентов автоматизированных систем • Регистрировать события, связанные с защитой информации в автоматизированных системах

профессиональных задач, профессионального и личностного развития. - Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. - Ориентироваться в условиях частой смены технологий в профессиональной деятельности. - Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий	распорядительные документы по системе защиты информации автоматизированной системы - Выявление угроз безопасности информации в автоматизированных системах - Принятие мер защиты информации при выявлении новых угроз безопасности информации - Анализ недостатков в функционировании системы защиты информации автоматизированной системы - Устранение недостатков в функционировании системы защиты информации автоматизированной системы	- Анализировать события, связанные с защитой информации в автоматизированных системах - Классифицировать и оценивать угрозы информационной безопасности - Контролировать события безопасности и действия пользователей автоматизированных систем

Оценка качества освоения учебных модулей проводится в процессе промежуточной аттестации в форме тестирования.

Оценка	Критерии оценки
Зачтено	Оценка **«Зачтено»** выставляется слушателю, если он твердо знает материал курса, грамотно и по существу использует его, не допуская существенных неточностей в ответе на тестовые вопросы,. Не менее 70% правильных ответов при решении тестов.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который не знает значительной части программного материала, допускает существенные ошибки. Менее 70% правильных ответов при решении тестов.

Оценка качества освоения учебной программы проводится в процессе итоговой аттестации в форме ответов на теоретические вопросы и решения практических задач.

Оценка (стандартная)	**Требования к знаниям**
Зачтено	Оценка **«Зачтено»** выставляется слушателю, продемонстрировавшему твердое и всестороннее знание материала, умение применять полученные в рамках занятий практические навыки и умения, знание и умение применять теоретические положения при решении практических вопросов, владеет необходимыми навыками и приемами их выполнения. Достижения за период обучения и результаты промежуточной аттестации демонстрировали отличный уровень знаний и умений слушателя. Не менее 70% правильных ответов на теоретические вопросы и правильных решений практических задач.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который в недостаточной мере овладел теоретическим материалом по дисциплине, допустил ряд грубых ошибок при выполнении практических заданий, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно, а также не выполнил требований, предъявляемых к промежуточной аттестации. Достижения за период обучения и результаты промежуточной аттестации демонстрировали неудовлетворительный уровень знаний и умений слушателя. Менее 70% правильных ответов на теоретические вопросы и правильных ответов при решении практических задач.

Фонд оценочных средств

Оценочные материалы

ТЕСТОВЫЕ ВОПРОСЫ

Дисциплина «Внедрение и техническая поддержка InfoWatch Traffic Monitor»

Архитектура и технологии InfoWatch Traffic Monitor

1. Какая задача решается с помощью Infowatch Data Discovery?
   - Получение данных находящихся в покое: из сетевых хранилищ, Share Point и с локальных дисков рабочих станций пользователей.
   - Визуальный анализ и формирование представления данных в любом разрезе.
   - Получение данных с рабочих станций пользователей.
   - Получение данных с почтового сервера, Proxy сервера и span порта, а так же, от других систем. Настройка, обработка, анализ и применение политик защиты данных.
2. Какие технологии анализа работают непосредственно на агенте Device Monitor?
   - Лингвистический анализ
   - Детектор текстовых объектов
   - Детектор эталонных документов
   - Детектор заполненных бланков
   - Детектор эталонных печатей
   - Детектор выгрузок из баз данных
   - Детектор графических объектов
   - Автолингвист
3. Какой почтовый сервер устанавливается совместно с Traffic Monitor и используется для отправки сообщений получателю или следующему relay-серверу в почтовой системе?
   - Microsoft Exchange Server
   - Sendmail

- Postfix
- Exim
- Qmail
- Apache James server

4. По каким протоколам может быть перехвачена информация, поступающая со SPAN порта соответствующего сетевого оборудования на сервер Traffic Monitor?
   - HTTP
   - HTTPS
   - FTP
   - FTPS
   - SMTP
   - POP3
   - IMAP
   - NRPC
   - NRPC/SSL
   - MAPI
   - XMPP
5. Какая компонента Traffic Monitor отвечает за прием данных со SPAN порта?
   - iw_sniffer
   - iw_capstack
   - iw_messed
   - iw_analysis
6. Какая компонента Traffic Monitor отвечает за прием данных с Proxy сервера?
   - iw_proxy_smtp
   - iw_proxy_http
   - iw_icap
   - iw_xapi
7. Какую функцию выполняет компонента iw_warpd?
   - извлекает данные из контейнеров, вложенных в перехваченные объекты
   - определяет наличие объекта защиты и добавляет объекту соответствующие атрибуты
   - запускает по порядку все технологии анализа, которые установлены в системе
   - применяет политики к перехваченным объектам
8. При реализации филиальной структуры, какой сервер может быть только один (без вспомогательной или дополнительной ноды)?
   - База данных Traffic Monitor
   - Traffic Monitor
   - Active Directory
   - Device Monitor
   - База данных Device Monitor
9. Как Traffic Monitor получает объекты от Device Monitor и Data Discovery, а также внешних систем?
   - через адаптеры по thrift-интерфейсу
   - по протоколу ICAP
   - по протоколу MIME
   - по SPAN протоколу
10. К какому внутреннему формату приводятся объекты в Traffic Monitor?
    - XML+DAT
    - MIME
    - EML
    - XML

- DAT
- EML+ DAT

Развертывание InfoWatch Traffic Monitor

1. Какая программа используется для получения сведений о статусе процессов ТМ, сбора статистики и отправки уведомлений администратору сервера?
    - Zabbix
    - Nagios
    - Sensu
    - Icinga
2. Автоматическое удаление событий из БД…
    - включено по умолчанию и может быть изменено в процессе установки, период хранения может быть установлен индивидуально для событий разного типа (с нарушениями, без нарушений, хранение скриншотов)
    - включено по умолчанию и не может быть изменено в процессе установки
    - выключено по умолчанию и не может быть изменено в процессе установки
    - включено по умолчанию и может быть изменено в процессе установке, период хранения устанавливается одинаковым для всех типов событий (с нарушениями, без нарушений, хранение скриншотов)
3. Параметр установки ТМ «Daily tablespace paths» определяет…
    - путь к диску хранения данных ежедневного табличного пространства
    - путь к диску хранения данных основного табличного пространства
    - количество путей для файлов ежедневных табличных пространств
    - путь к диску хранения файлов архивированных табличных пространств
4. Какая децентрализованная отказоустойчивая система обнаружения сервисов (Service Discovery) используется в ТМ для регистрации сервисов, мониторинга доступности и обнаружения компонент?
    - Consul
    - Redis
    - Etcd
    - ZooKeeper
    - Doozerd
5. Какие предлагаются варианты указания NTP-сервера при установке ТМ?
    - Use system NTP-server
    - DHCP
    - Set manually
    - PROXY

Развертывание InfoWatch Device Monitor for Windows

1. На какие операционные системы может быть установлен агент Device Monitor версии 7.11?
    - Microsoft Windows 7 Service Pack 1 и выше
    - Microsoft Windows Server 2008 R2 и выше
    - РЕД ОС 7.3
    - Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"
    - Альт Рабочая станция 10
    - MacOS 10.14 и выше
    - Red Hat Enterprise Linux 7.0 и выше
2. Ключ шифрования (ключ защищенного канала) Device Monitor…
    - создается при установке Основного сервера, далее указывается при установке Вспомогательных серверов

- создается отдельно для каждой ноды сервера Device Monitor, т.е. отдельно для Основного сервера и каждого из Вспомогательных серверов
- запрашивается в службе технической поддержки компании «Инфовотч» и указывается при установке как Основного, так и Вспомогательных серверов Device Monitor
- запрашивается в службе технической поддержки компании «Инфовотч» отдельно для каждой ноды сервера Device Monitor, т.е. отдельно для Основного сервера и каждого из Вспомогательных серверов

3. Ключ шифрования (ключ защищенного канала) Device Monitor необходим для…
    - обнаружения сервером агентов, ранее установленных на рабочих станциях
    - шифрования данных, которые передаются с сервера Device Monitor на сервер Traffic Monitor
    - шифрования данных, которые передаются с сервера Traffic Monitor на сервер Device Monitor
    - шифрования данных, которые передаются между агентом Device Monitor и сервером Device Monitor
    - обнаружения агентами всех доступных серверов в своем окружении
    - шифровании данных, которые передаются между сервером Device Monitor и базой данных
4. Как получить сертификат web-сервераTraffic Monitor?
    - запросить в службе технической поддержки
    - скопировать с сервера, где установлен Traffic Monitor файл /opt/iw/tm5/etc/web.conf
    - на сервере, где установлен Traffic Monito открыть файл /opt/iw/tm5/etc/xapi.conf, в секции "ThriftServers -> xapi", в параметре "TrustedCertificatesPath" будет указано расположение и имя файла с сертификатом web-сервераTraffic Monitor
    - выполнить экспорт файла сертификата из web-браузера где открыта консоль управления Traffic Monitor
5. Конфигурация Блокады приложений...
    - настраивается специалистом исключительно самостоятельно
    - загружается из соответствующего файла, который входит в поставку системы
    - загружается из соответствующего файла, который необходимо запросить в технической поддержке
    - может быть загружена из соответствующего файла, который приобретается дополнительно

Администрирование InfoWatch Traffic Monitor

1. Какая команда выполняет «мягкую» остановку процесса cas?
    - iwtm kill cas
    - iwtm remove cas
    - iwtm stop cas
    - iwtm delete cas
    - iwtm disable cas
2. Выполнение команды iwtm status cas отобразило статус компоненты «inactive (dead) loaded (enabled)» это означает что…
    - компонента загружена и запущена
    - компонента загружена, но не запущена
    - компонента не загружена и не запущена
    - компонента не доступна для загрузки и запуска
3. Какие опции доступны для команды «iwtm»?
    - reload
    - reboot

- test
- disable
- run
- activate
- shutdown

4. В каком каталоге находятся конфигурационные файлы системы Traffic Monitor?
    - /etc
    - /opt/iw/tm5/bin
    - /opt/iw/tm5/etc
    - /opt/iw/tm5/queue/
    - /var/log/infowatch/
5. В каком каталоге находятся очереди обработки объектов системы Traffic Monitor?
    - /opt/iw/tm5/queue/
    - /opt/iw/tm5/etc
    - /opt/iw/tm5/bin
    - /u01/postgres
    - /u02/pgdata
6. Какой скрипт позволяет удалить временные файлы Traffic Monitor?
    - opt/iw/tm5/bin/clean_temporary_files.sh
    - /opt/iw/tm5/bin/iw_qtool
    - /opt/iw/tm5/bin/iw_vademcum
    - /opt/iw/tm5/bin/iw_tech_tools
7. Какие опции доступны для скрипта «iw_qtool»?
    - move
    - remove
    - delete
    - clean
    - put
    - stat
    - erase
    - load
8. Как вывести на экран в реальном времени информацию о работе базы данных PostgreSQL?
    - tail –f /u01/postgres/pg_log/postgresql.log
    - tail -f /var/log/messages
    - tail -f /var/log/syslog
    - tail -f /var/log/pgagent-9.6.log
9. Какую команду необходимо выполнить для того, чтобы установить срок хранения событий с нарушениями равным 60 дней для СУБД Postgres?
    - ./dbconf-iwdrop-postgres.sh set violation 60
    - ./dbconf-iwdrop-postgres.sh set noviolation 60
    - ./dbconf-iwdrop-postgres.sh set other 60
    - ./dbconf-iwdrop-postgres.sh set screenshot 60
10. В каком файле устанавливается минимальный и максимальный размер растровых изображений (графических файлов), к которым будет применяться OCR Google Tesseract?
    - /opt/iw/tm5/etc/image2text_ts.conf
    - /opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml
    - /opt/iw/tm5/etc/sample_compiler.conf
    - /opt/iw/tm5/etc/warpd.conf

Развертывание InfoWatch Device Monitor for Linux

1. Какая колоночная аналитическая СУБД используется для работы web консоли Device Monitor for Linux?
    - Vertica
    - ParAccel
    - ClickHouse
    - Greenplum Database
    - Sybase IQ
    - Kognito
2. Какое средство управления кластером контейнеров используется для работы web консоли Device Monitor for Linux?
    - Kubernetes
    - OpenShift
    - Salt
    - Vagrant
    - Rancher
3. Какая реляционная СУБД используется для работы сервера Device Monitor for Linux?
    - PostgresSQL
    - Oracle
    - DB2
    - MS SQL Server
    - MySQL
4. Как получить токен шифрования трафика обмена данными между сервером Device Monitor for Linux и сервером Traffic Monitor?
    - запросить в службе технической поддержки компании «Инфовотч»
    - приобрести дополнительно у компании «Инфовотч»
    - скопировать из файла token.conf
    - скопировать через web консоль Traffic Monitor: Управление -> Плагины -> Device Monitor -> Токены -> Скопировать токен
5. Как указать к какому серверу Device Monitor for Linux должен подключаться агент Device Monitor for Linux в случае его локальной установки на рабочей станции?
    - указать ip адрес или доменное имя сервера Device Monitor for Linux в процессе интерактивной установки агента
    - указать ip адрес или доменное имя сервера Device Monitor for Linux в качестве параметра при запуске скрипта установки агента
    - указать ip адрес или доменное имя сервера Device Monitor for Linux через web-консоль управления настройками агента Device Monitor for Linux после его установки
    - никак не указывать, сервер Device Monitor for Linux самостоятельно обнаруживает компьютеры, на которые установлен агент

Развертывание InfoWatch Vision

1. Какая колоночная аналитическая СУБД используется для работы web консоли Device Monitor for Linux?
    - Vertica
    - ParAccel
    - ClickHouse
    - Greenplum Database
    - Sybase IQ
    - Kognito

2. Какое средство создания контейнеров используется для работы Vision?
    - RKT
    - PodMan
    - OpenVZ

- Nanobox
- Docker
- Singularity

3. Как получить файл плагина Vision для его загрузки в Traffic Monitor?
    - запросить в службе технической поддержки компании «Инфовотч»
    - приобрести дополнительно у компании «Инфовотч»
    - скопировать /vision/tmplugin/vision.zip с сервера, где установлена система Vision (в директории /vision) на компьютер где запущена web-консоль Traffic Monitor
    - скопировать файл из каталога установки системы после распаковки архива iw_vision_setup_2.3.X.xxxx.tar.xz (файл поставляется вместе с дистрибутивом системы Vision)
4. Как проверить, развернуты ли поды (PODS), реализующие «бизнес-логику» системы Vision?
    - # systemctl status kubelet
    - # kubectl cluster-info
    - # kubectl get pods -o wide -n kube-system
    - # kubectl get pods -o wide -n infowatch
5. Какая команда выполняет сброс установки системы Vision?
    - # ./setup.py cancel
    - # ./setup.py undo
    - # ./setup.py reset
    - # ./setup.py remove
    - # ./setup.py update
    - # ./setup.py delete

Развертывание InfoWatch Data Discovery

1. Какую команду следует использовать для удаления всех сторонних компонентов системы таких как Docker, Kubernetes и др., в случае если установка продукта прервалась или продукт был установлен некорректно?
    - ./setup.py remove
    - ./setup.py reset
    - ./setup.py install
    - ./setup.py showproducts
2. Какой пакет необходимо дополнительно скачать и установить для корректной работы, используемого в InfoWatch Data Discovery - Docker 19.03 в окружении Oracle Linux и Red Hat Enterprise Linux 7?
    - containerselinux - 2.107-1.el7_6.noarch.rpm
    - iw_am_setup_1.0.0.xxx.tar.xz
    - pmilter-x-1.4-0.el6.x86_64.rpm
    - bash-4.1.2-15.el6_5.2.x86_64.rpm
    - pg_pathman96-1.5.2-4.el6.x86_64.rpm
3. Программа установки InfoWatch Data Discovery написана на языке Python версии 2.7. Нужно ли устанавливать интерпретатор этого языка или пакет с интерпретатором входит в состав дистрибутива продукта?
    - Нет, не нужно устанавливать интерпретатор языка Python версии 2.7, т.к. он входит в дистрибутив продукта
    - Да, нужно устанавливать интерпретатор языка Python версии 2.7, т.к. он не входит в дистрибутив продукта
4. Начиная с какой версии InfoWatch Traffic Monitor (TM) поддерживается синхронизация InfoWatch Data Discovery?
    - начиная с версии TM 7.0.1
    - начиная с версии TM 6.11.3

- начиная с версии TM 6.10.15
- начиная с версии TM 6.7.12

5. В каких браузерах официально поддерживается работа офицера безопасности?
    - Google Chrome
    - Opera
    - Firefox Browser
    - Яндекс.Браузер
    - Tor Browser
6. На каких операционных системах официально поддерживается работоспособность продукта InfoWatch Data Discovery?
    - Astra Linux Special Edition 1.7.x "Смоленск"
    - Microsoft Windows 8
    - Microsoft Windows Server 2016
    - Microsoft Windows Server 2019
    - Ubuntu 20.10 “Groovy Gorilla”
    - CentOS Linux 7 и более поздние
    - Red Hat Enterprise Linux 7.7 и более поздние
    - Oracle Linux 7.9 и более поздние
    - RedOS 7.3.1
    - ОС Альт
7. Какие варианты установки и размещения имеет InfoWatch Data Discovery (DD)?
    - Возможна совместная установка на одном сервере с TM
    - Только установка на отдельном сервере
    - Только совместная установка DD на одном сервере с TM
    - Возможна установка DD на одном сервере с другими продуктами InfoWatch, такими как Vision и Activity Monitor, либо на отдельном сервере
8. Нужно ли перед установкой InfoWatch Data Discovery (DD) отключить межсетевой экран?
    - Ни в коем случае нельзя отключать межсетевой экран. При отключении межсетевого экрана, после установки, DD может быть неработоспособен
    - Нет, это необязательно. Межсетевой экран никоем образом не влияет на работу DD.
    - Да, нужно отключить межсетевой экран или настроить правила POD сети. В противном случае, после установки, DD может быть неработоспособен.

Развертывание InfoWatch Activity Monitor

1. Нужно ли перед установкой InfoWatch Activity Monitor (AM) отключить межсетевой экран?
    - Ни в коем случае нельзя отключать межсетевой экран. При отключении межсетевого экрана, после установки, AM может быть неработоспособен
    - Нет, это необязательно. Межсетевой экран никоем образом не влияет на работу AM.
    - Да, нужно отключить межсетевой экран или настроить правила POD сети. В противном случае, после установки, AM может быть неработоспособен.
2. Программа установки InfoWatch Activity Monitor написана на языке Python версии 2.7. Нужно ли устанавливать интерпретатор этого языка или пакет с интерпретатором входит в состав дистрибутива продукта?
    - Нет, не нужно устанавливать интерпретатор языка Python версии 2.7, т.к. он входит в дистрибутив продукта
    - Да, нужно устанавливать интерпретатор языка Python версии 2.7, т.к. он не входит в дистрибутив продукта
3. Какой пакет необходимо дополнительно скачать и установить для корректной работы, используемого в Infowatch Activity Monitor, Docker 19.03 в окружении Oracle Linux и Red Hat Enterprise Linux 7?
    - containerselinux - 2.107-1.el7_6.noarch.rpm

- iw_am_setup_1.0.0.xxx.tar.xz
- pmilter-x-1.4-0.el6.x86_64.rpm
- bash-4.1.2-15.el6_5.2.x86_64.rpm
- pg_pathman96-1.5.2-4.el6.x86_64.rpm

4. В каких браузерах официально поддерживается работа офицера безопасности?
    - Google Chrome
    - Opera
    - Firefox Browser
    - Яндекс.Браузер
    - Tor Browser
5. Какая СУБД используется в Infowatch Activity Monitor?
    - PostgreSQL 12
    - Oracle Database 12
    - Microsoft SQL Server 2005
    - Microsoft SQL Server 2008
    - Microsoft SQL Server 2012
    - Microsoft SQL Server 2014
    - Microsoft SQL Server 2016
    - PostgreSQL 9
6. На какую операционную систему может быть установлен Infowatch Activity Monitor?
    - Astra Linux Special Edition 1.6 "Смоленск"
    - Red Hat Enterprise Linux 7.5 и более поздние
    - Oracle Linux 7.0 и более поздние
    - Microsoft Windows 7 Service Pack 2
    - Microsoft Windows 8
    - Microsoft Windows Server 2016
    - Microsoft Windows Server 2019
    - Ubuntu 20.10 “Groovy Gorilla”
    - CentOS Linux 7 и более поздние
7. Начиная с какой версии Infowatch Traffic Monitor (TM) поддерживается синхронизация Infowatch Activity Monitor?
    - начиная с версии TM 6.10.10
    - начиная с версии TM 7.0.1
    - начиная с версии TM 6.11.3
    - начиная с версии TM 6.7.12
8. Какие варианты установки Infowatch Activity Monitor (AM) возможны относительно Infowatch Vision (Vision)?
    - возможна установка AM на отдельный сервер
    - возможна установка AM к уже имеющемуся Vision
    - возможна установка AM только на отдельный сервер
    - возможна установка AM только к уже имеющемуся Vision
9. Какие варианты установки и размещения имеет InfoWatch Activity Monitor (AM) относительно сервера Infowatch Traffic Monitor (TM)?
    - возможна установка AM на выделенном сервере для работы с одним или несколькими серверами TM (stand-alone)
    - возможна установка на одном сервере с TM
    - возможна только совместная установка AM на одном сервере с TM
    - возможна установка AM только на выделенном сервере для работы с одним или несколькими серверами TM (stand-alone)

10. Расставьте действия по установке системы Infowatch Activity Monitor (AM) в правильном порядке (в ответе укажите последовательность из цифр через запятую, например - 3, 2, 5, 1, 4 и т.д.):
    1. Скопировать архив с набором бинарных модулей образов контейнеров, необходимых для развертывания AM в созданную директорию
    2. Указать путь и выделить объем дискового пространства для размещения данных Clickhouse, Tarantool, PostgreSQL и для хранения данных
    3. Запустить программу интерактивной установки AM
    4. Дождаться окончания процесса установки
    5. Установить ОС
    6. Ознакомиться с условиями лицензионного соглашения
    7. Указать порт подключения к веб-интерфейсу
    8. Создать целевую директорию на диске
    9. Выделить объем оперативной памяти для размещения данных Clickhouse

Развертывание InfoWatch Prediction

1. Как получить файл плагина InfoWatch Prediction для его загрузки в Infowatch Traffic Monitor?
    - запросить в службе технической поддержки компании «Инфовотч»
    - приобрести дополнительно у компании «Инфовотч»
    - скопировать с сервера, где установлен Prediction, файл /tmplugin/prediction.zip из каталога, куда был распакован архив дистрибутива
    - скопировать с сервера, где установлен Prediction, файл prediction.zip из каталога где размещен архив iw_prediction_setup_x.x.x.xx.tar.gz
2. Как проверить, развернуты ли поды (PODS), реализующие «бизнес-логику» системы Infowatch Prediction?
    - # systemctl status kubelet
    - # kubectl cluster-info
    - # kubectl get pods -o wide -n kube-system
    - # kubectl get pods -o wide -n infowatch
3. За какой минимальный период времени до интеграции Infowatch Prediction с Infowatch Traffic Monitor должна быть импортирована соответствующая конфигурация в Infowatch Traffic Monitor?
    - одна неделя
    - две недели
    - один месяц
    - два месяца
4. Для корректного расчета рейтинга по каким группам риска Infowatch Prediction необходимы данные из Infowatch Traffic Monitor с заранее импортированной конфигурацией?
    - Подготовка к увольнению
    - Нелояльные сотрудники
    - Аномальный вывод информации
    - Нетипичные внешние коммуникации
    - Отклонение от бизнес-процессов
5. Какое средство создания контейнеров используется для работы Infowatch Prediction?
    - RKT
    - PodMan
    - OpenVZ
    - Nanobox
    - Docker
    - Singularity

6. Начиная с какой версии InfoWatch Traffic Monitor возможна интеграция с Infowatch Prediction?
    - InfoWatch Traffic Monitor 6.10
    - InfoWatch Traffic Monitor 6.11
    - InfoWatch Traffic Monitor 7.0
    - InfoWatch Traffic Monitor 7.1
    - InfoWatch Traffic Monitor 7.2
    - InfoWatch Traffic Monitor 7.3
7. Какой пакет необходимо предварительно установить перед запуском инсталляции Infowatch Prediction?
    - container-selinux
    - rpmfusion
    - tcpdump
    - yum-plugin-fastmirror
8. На каком языке программирования написана программа установки Infowatch Prediction и для ее запуска должен быть установлен соответствующий интерпретатор?
    - Python 2.7
    - C/C++
    - Java 13
    - Java 13
    - JavaScript
9. На какую операционную систему может быть установлен Infowatch Prediction?
    - Astra Linux Special Edition 1.6, 1.7 «Smolensk»
    - Red Hat Enterprise Linux, версии 7.x (7.7 и выше) и 8.x (8.0 и выше)
    - РЕД ОС 7.x.x (начиная с 7.3.1)
    - Oracle Linux версии 7.x (7.9 и выше) и 8.x (8.4 и выше)
    - Astra Linux Common Edition «Орел» версия 2.12 (x64) с версией ядра 4.15 и выше
    - Debian Linux 9 и выше
    - Microsoft Windows Server 2016 и выше
10. Какой допустим вариант установки Infowatch Prediction относительно сервера Infowatch Traffic Monitor (TM) и других продуктов Infowatch?
    - установка Prediction на отдельном сервере либо совместная установка с Infowatch Data Discovery 1.5.1 и выше или с Infowatch Vision 2.8 и выше
    - возможна установка Prediction на одном сервере с TM
    - установка Prediction только на одном сервере с TM
    - возможна установка Prediction на одном сервере с любыми другими продуктами InfoWatch кроме TM
    -

Дисциплина «Обзор аналитических работ»

1. Отметьте достоинства метода выявления требований «Интервью»:
    - произвольная последовательность вопросов
    - использование вспомогательных материалов
    - быстрое получение первичной информации
    - минимальные затраты времени на общение
    - возможность получения одинаковых ответов от интервьюируемых

2. Отметьте способы, с помощью которых в процессе интервью можно получить наиболее полную информацию:
    - менять порядок заготовленных вопросов, исключать одни вопросы и добавлять другие
    - менять формулировку вопроса если интервьюируемому вопрос не понятен

- вести заметки
- предварительно выслать перечень вопросов
- четко следовать подготовленному плану интервью
- строго соблюдать порядок и формулировку заготовленных вопросов
- назначить удобное вам время и формат проведения интервью

3. Какой из методов выявления требований является самым информативным?
    - Интервью
    - Опросный лист
    - Изучение документации
    - Самого информативного метода нет, каждый метод используется исходя из возможностей получения информации и поставленных задач

4. В каких случаях выявление требований на основе изучения документации является затруднительным либо его использование нецелесообразно?
    - в организации имеется только базовая документация
    - в организации полностью отсутствует базовая документация
    - в организации не поддерживается актуальность документации
    - заказчик может предоставить часть информации только в обезличенном виде, т.е. без конкретных данных, например, шапки таблиц, шаблоны документов
    - требуется быстрое получение информации

5. Определите, что целесообразно предпринять следующей ситуации. Вы должны взять интервью у руководителя подразделения, но он под различными предлогами избегает встречи. У вас есть основания полагать, что он не достаточно компетентен и страшится показать свою неосведомленность по существу рассматриваемых вопросов.
    - обратиться к вышестоящему руководителю с просьбой об оказании содействия в проведении интервью
    - предложить руководителю подразделения заполнить опросный лист и использовать его для определения требований
    - запросить у руководителя подразделения документацию и использовать ее для определения требований
    - предложить руководителю подразделения назначить сотрудника для проведения интервью (при условии, что сотрудник обладает всей полнотой необходимой информации)

6. Определите приоритетный метод выявления требований когда владельцем информации является руководитель управленческого подразделения (например, отдела ИБ).
    - Интервью
    - Опросный лист
    - Изучение документации

7. Определите приоритетный метод выявления требований для следующей ситуации. Очень крупная организация, имеет сложную иерархическую и территориально распределенную структуру. Данных о наличии регламентирующей документации и степени ее актуальности нет.
    - Интервью
    - Опросный лист
    - Изучение документации

8. При проведении интервью использование диктофона…

- недопустимо
- является обязательным
- обязательно требует получения письменного согласия, интервьюируемого и руководства организации
- необходимо предварительно согласовать с интервьюируемым, факт подтверждения согласия должен быт записан на диктофон в начале интервью

9. Выберите правильные утверждения, касающиеся использования технологии лингвистического анализа в ТМ
   - детектирование опечаток по умолчанию включено и отключить его нельзя
   - детектирование опечаток по умолчанию отключено, чтобы его включить нужно внести изменения в конфигурационный файл cas.conf
   - транслитерация по умолчанию включена и отключить ее нельзя
   - транслитерация по умолчанию отключена, чтобы ее включить нужно внести изменения в конфигурационный файл cas.conf
   - учет морфологии по умолчанию включен для всех терминов и отключить его нельзя
   - учет морфологии по умолчанию отключен для всех терминов чтобы его включить нужно внести изменения в конфигурационный файл cas.conf
   - учет морфологии настраивается для каждого термина

10. Отметьте основные технологии, реализованные в IW TM (всегда включаются в поставку)
    - Лингвистический анализ
    - Текстовые объекты
    - Эталонные документы
    - Бланки
    - Печати
    - Выгрузки из баз данных
    - Графические объекты
    - Автолингвист

Дисциплина «Правовые и организационные аспекты легитимизации DLP системы»

1. На основание каких доводов работник может опротестовать свое увольнение в суде?
   - Не установлен факт пересылки конфиденциальной информации
   - Не все регламентирующие документы, принятые в компании, были им подписаны
   - Сотрудник не знал, какая информация является конфиденциальной
   - Его рабочей станцией мог воспользоваться другой сотрудник
   - Работники не был осведомлен, что в компании ведется мониторинг и контроль
2. В какой срок, компания должна получить объяснения от сотрудника, нарушившего политику информационной безопасности:
   - В этот же день
   - В течение трех рабочих дней
   - Не более двух дней
   - При формирование необходимого пакета документов при судебном разбирательстве
3. Относится ли IW Traffic Monitor к специальным техническим средствам, предназначенных для негласного получения информации?
   - Да, относится
   - Нет, не относится
   - Относятся только некоторые компоненты
   - Да, согласно постановлению Правительства от 10.03.2000 N 214
4. Какой документ необходимо утвердить в компании, где прописаны принципы и правила использование DLP-системы?

- Приказ о защите информации
- Положение о защите информации ограниченного доступа
- Дополнительное соглашение к трудовому договору между работником и организацией
- Регламент мониторинга и контроля

5. Имеет ли право сотрудник использовать в личных целях информационные ресурсы компании, если это не оговорено в трудовом договоре?
- Имеет
- Имеет, если это не запрещено другим актом
- Не имеет
- Имеет, после выполнения своих должностных обязанностей

6. Какое взыскание может быть наложено на работника, при нарушении правил трудового распорядка?
- Штраф
- Увольнение
- Выговор
- Замечание
- Депремирование

7. Необходима ли аттестация информационной системы и ввод её в действие?
- Да, обязательно
- Нет, не обязательно
- По желанию руководства компании
- По требованию надзорных органов

8. Какой приказ ФСТЭК утверждает требования о защите информации, не составляющей государственную тайну?
- Приказ ФСТЭК № 53
- Приказ ФСТЭК № 21
- Приказ ФСТЭК № 17
- Приказ ФСТЭК № 12

9. В чем заключаются обязательства сотрудника в целях охраны коммерческой тайны?
- Не разглашать информацию
- Не хранить информацию на внешнем носителе
- Не сообщать пароль от своего логина для входа на рабочую станцию
- Возместить причиненные убытки работодателю

10. Могут ли операторы или иные лица, получившие персональные данные, передавать их третьим лицам?
- Могут
- Не могут
- Могут с согласия субъекта персональных данных
- Могут по решению суда

Дисциплина «Настройка и использование программных средств Infowatch»

1. Какой режим создания запроса позволяет создать гибкую настройку параметров запроса?
- Расширенный
- Обычный
- Детальный
- Пользовательский

2. Какой раздел отчетности используются для оперативного получения статистических данных?
- Сводка
- События
- Отчеты

- Выгрузки

3. Как определяется время перехвата события?
   - Время перехвата события - это локальное время на агенте Device Monitor, где осуществляется перехват
   - Время перехвата события - это локальное время на сервере Device Monitor
   - Время перехвата события - это локальное время на сервере Traffic Monitor
   - Время перехвата события - это глобальное время системе Infowatch Traffic Monitor
4. Какие фильтры доступны для поиска персон и компьютеров?
   - Фильтр наличия снимков экрана
   - Фильтр выбора персон и компьютеров с определенным статусом
   - Поле поиска
   - Фильтр даты создания карточки персоны или компьютера
5. Какая группа политик отрабатывает непосредственно на агенте Infowatch Device Monitor?
   - Политика защиты данных
   - Политика защиты данных на агенте
   - Политика контроля персон
   - Политика хранения
6. Каким образом можно запретить запуск определенного программного обеспечения для пользователя?
   - Создать список Приложений
   - Создать правило Application Monitor
   - Назначить политику, содержащую правило запрета на группу сотрудников
   - Назначить политику, содержащую правило запрета на группу компьютеров
   - Создать Белый список
   - Создать правило Device Monitor
   - Создать правило File Monitor
7. В каком разделе консоли управления Device Monitor можно управлять списками устройств, доступ к которым безусловно разрешен?
   - Белые списки
   - Приложения
   - Политики
   - Группы компьютеров
8. Каким образом можно назначить созданную политику?
   - Созданную политику можно назначить через редактирование группы сотрудников
   - Созданную политику можно назначить через редактирование группы компьютеров
   - Назначить, на кого будет действовать созданная политика, можно в разделе Политики
   - Назначить, на кого будет действовать созданная политика, можно в разделе Политики
9. Где можно собрать диагностическую информацию по работе агента Device Monitor удаленно?
   - В разделе Группы компьютеров
   - В разделе Группы сотрудников
   - Диагностическую информацию по работе агента можно собрать только локально на рабочей станции, где установлен агент
   - Диагностическую информацию по работе агента можно собрать в логе приложении Windows
10. Какие приложения отображаются в протоколе приложений?
    - все приложения, установленные на рабочих станциях
    - все приложения, которые запускались на рабочих станциях
    - все приложения, которые запускались на рабочих станциях, кроме критичных для работы компьютера

- все приложения, которые запускались на рабочих станциях кроме указанных в перечне «Исключение приложений из перехвата»
- все приложения, которые запускались на рабочих станциях, кроме критичных для работы компьютера и указанных в перечне «Исключение приложений из перехвата»

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

1. Дисциплина «Подготовка и реализация Концепции Политики защиты данных»

1. Разработать Политику защиты данных для предложенной ситуации (кейса) согласно соответствующему шаблону.
2. Реализовать разработанную Политику защиты данных в системах Infowatch Traffic Monitor и Infowatch Device Monitor.
3. Оценить результаты работы реализованной Политики защиты данных, при необходимости выполнить доработку Политики.

Шаблон Политики защиты данных

1. Используемые технологии анализа.

перечислить технологии анализа, которые необходимо использовать для предотвращения утечки защищаемых данных

2. Объекты защиты (ОЗ)

№ п/п	Название ОЗ	Состав ОЗ

3. Списки отправителей/получателей

№ п/п	Название периметра	Список

4. Политики защиты данных

№ п/п	Название Политики	Тип политики	Объекты защиты	Правила срабатывания

5. Правила Device Monitor

перечислить правила, которые должны быть созданы в системе Device Monitor

Описание ситуаций (кейсов)

Кейс № 1

В последние полгода Агентство недвижимости «Удача» начало активно терять клиентов, также некоторые девелоперы, представляющие квартиры в новостройках стали отказываться от сотрудничества и отзывать сделанные предложения.

Проведенное расследование показало, что за указанный период в агентство начали активно приходить менеджеры по продажам-стажеры, которые после получения доступа к данным скачивали нужную информацию и внезапно увольнялись. Опрос ушедших клиентов показал, что они получили более выгодные предложения от конкурирующего агентства недвижимости «Мечта».

Для того, чтобы предотвратить подобные инциденты в будущем, была куплена DLP система и приглашен аналитик для ее настройки под требования заказчика.

Необходимо обеспечить контроль:

- передачи на внешние почтовые адреса данных, касающихся объектов недвижимости: информация о стоимости квартир, основные параметры квартир (адрес, этаж, площадь, количество комнат, состояние), сведения об инфраструктуре (расположение парковок, детских садов, больниц, школ) и так далее
- передачи или копирования планов квартир

Необходимо исключить:

- передачу, копирование или печать информации из базы клиентов
- возможность снятия скриншотов при работе с базой клиентов

При этом следует вести особый контроль для новых сотрудников и обеспечить оперативное информирование офицера безопасности об инцидентах с их участием.

Кейс № 2

Совсем недавно у компании ООО «Товары.ру» начались проблемы с поставщиками, некоторые из них решили отказаться от сотрудничества по причине низкой закупочной цены. Также с недавнего времени один из главных конкурентов - ООО «Ценопад начал открывать свои новые магазины через неделю после открытия точек ООО «Товары.ру», но в более удобных для потребителей местах (например, ближе к метро).

Служба информационной безопасности провела расследование, в результате которого стало ясно, что злоумышленником является бывший сотрудник компании, который теперь работает в компании конкурентов ООО «Ценопад». Служба ИБ предполагает, что при увольнении он смог забрать с собой части баз данных, которые содержали информацию о поставщиках и входящих закупочных ценах. Для того чтобы предотвратить подобные инциденты в будущем, была куплена DLP система и приглашен аналитик для ее настройки под требования заказчика.

У бывшего сотрудника осталось несколько хороших знакомых в компании ООО «Товары.ру», которые могли передать информацию об открытии магазинов, персональных данных квалифицированных сотрудников и потенциально продолжают помогать ему. Сотрудникам службы безопасности известен круг общения бывшего сотрудника, и им хотелось бы предотвратить дальнейшие возможные утечки информации. ООО «Ценопад» не единственный конкурент на рынке, поэтому сотрудники службы ИБ высказали пожелание контролировать любые контакты и с другими конкурирующими торговыми сетями.

Кейс № 3

Одна из сотрудниц банка «SuperCredit» отправила около 20 кредитных историй клиенту банка вместо бюро. С ее стороны это были непреднамеренные действия. Девушка ошиблась, нажав ответить в сообщении клиента, вместо того чтобы ответить на сообщение-запрос из бюро. Таким образом, клиент получил не только свою кредитную историю, но и персональные данные (ФИО, серия и номер паспорта, ИНН, страховой номер ПФР) других клиентов банка. Данные клиентов оказались скомпрометированы в результате неумышленной утечки.

Сотрудница сразу же обратилась в службу ИБ, объяснив ситуацию. Данная ситуация произошла в банке впервые. Для того чтобы предотвратить подобные инциденты в будущем, была куплена DLP система и приглашен аналитик для ее настройки под требования заказчика.

Начальник ИБ считает, что необходимо контролировать отдел кредитования на предмет массовой передачи персональных данных на внешние адреса (за исключением бюро) и копирование на внешние устройства. В случае попыток массовой передачи или копирования должна происходить блокировка.

Кейс № 4

Несколько дней назад в СМИ появилась информация о том, что у нефтяной компании ООО «Нефтедобыча» готовится к заключению контракта с партнером АО «НПЗ». Сумма сделки, чертежи с трассами нефтепроводов и карты месторождений попали в открытый доступ. В результате преждевременного раскрытия информации, партнер отказался от заключения контракта. В результате инцидента ООО «Нефтедобыча» понесла финансовые потери, а также была признана ненадежным партнером.

Служба информационной безопасности провела расследование, в результате которого стало ясно, что злоумышленник находится внутри компании. Для того чтобы предотвратить подобные инциденты в будущем, была куплена DLP система и приглашен аналитик для ее настройки под требования заказчика.

Начальник ИБ имеет четкое понимание о том, что потенциальные нарушители могут быть среди отдела инженерного проектирования, управления технологий инжиниринга и бурения и оперативно-аналитического отдела. Имеются на руках примеры документации, чертежей, карт,

которые были переданы в открытый доступ. Подобная информация в рамках рабочих процессов может передаваться только сотрудникам организаций ООО «Нефтьстрой», ПАО «Нефтепром».

Начальник настроен очень серьезно и планирует блокировать все потенциальные утечки информации.

ВОПРОСЫ И ЗАДАНИЯ К ЗАЧЕТУ

Теоретические вопросы

1. Назначение и принципы работы системы Infowatch Traffic Monitor и его модулей Infowatch Device Monitor, Infowatch Data Discovery, Infowatch Vision.
2. Аппаратные и программные требования к системе Infowatch Traffic Monitor и его модулям Infowatch Device Monitor, Infowatch Data Discovery, Infowatch Vision.
3. Назначение и принципы работы основных служб Traffic Monitor.
4. Назначение ежедневных табличных пространств и параметры их настройки.
5. Режимы хранения данных Traffic Monitor.
6. Способы установки агента Device Monitor на рабочую станцию.
7. Принцип работы и порядок переключения режимов "черного" и "белого" списка приложений Device Monitor.
8. Назначение и принципы работы белого списка устройств Device Monitor.
9. Возможности перехвата информации системой Traffic Monitor (с каких устройств, по каким протоколам).
10. Способы формирования списка приложений Device Monitor.
11. Методы сбора требований: перечень, возможности, особенности использования.
12. Метод сбора требований – интервью, возможности и ограничения метода, способы повышения эффективности использования.
13. Метод сбора требований – опросный лист, возможности и ограничения метода, способы повышения эффективности использования.
14. Метод сбора требований – изучение документации, возможности и ограничения метода, способы повышения эффективности использования.
15. Организация процесса сбора требований.
16. Технология «Лингвистический анализ»: назначение, возможности, принципы работы.
17. Технология «Текстовые объекты»: назначение, возможности, принципы работы.
18. Технология «Эталонные документы»: назначение, возможности, принципы работы.
19. Технология «Бланки»: назначение, возможности, принципы работы.
20. Технология «Печати»: назначение, возможности, принципы работы.
21. Технология «Выгрузки из баз данных»: назначение, возможности, принципы работы.
22. Технология «Графические объекты»: назначение, возможности, принципы работы.
23. Технология «Автолигвист»: назначение, возможности, принципы работы.
24. Порядок подготовки данных для формирования Политики защиты данных
25. Содержание и элементы Политики защиты данных.
26. Федеральное законодательство РФ в сфере защиты информации.
27. Ответственность сотрудников за утечку данных.
28. Порядок привлечения к ответственности сотрудников, виновных в утечке данных.
29. Организационное обеспечение использования системы защиты от утечки данных.
30. Нормативно-правовое обеспечение использования системы защиты от утечки данных.

Практические задания

Практические задания по системе IW Traffic Monitor

1. Создать объект защиты, который обнаруживается в системе в случае нахождения категории «Финансы» и текстового объекта «ИНН» от 3-х вхождений.
2. Создать объект защиты, который обнаруживается в системе в случае обнаружения категории «Информация по счетам» или текстового объекта «БИК» или эталонного бланка «Выписка по счету» (от 5-ти заполненных полей).
3. Настроить политику с высоким уровнем нарушения при копировании на съемные устройства презентаций, отражающих информацию о стратегии компании.

4. Настроить политику со средним уровнем нарушения при обнаружении документов с грифами конфиденциальности на рабочих станциях сотрудников.
5. Настроить политику с высоким уровнем нарушения и тегом «На рассмотрение» при отправке по личной почте номеров кредитных карт в количестве от 5 штук.
6. Назначить на любых трех сотрудников статус «Под подозрением» и настроить на сотрудников с данным статусом политику контроля персон – отправка почтового уведомления офицеру безопасности при выполнении персоной действий с высоким уровнем нарушения.
7. Настроить политику контроля использования буфера обмена для сотрудников имеющих статус «Под подозрением» и присвоения высокого уровня нарушения соответствующим событиям.
8. Добавить в карточку любой персоны еще один рабочий контакт.
9. Создать группу «Отдел кадров», внести туда несколько персон. Настроить политику таким образом, чтобы при отправке любой информации на веб-ресурсы из списка «Поиск работы» для любого сотрудника, кроме группы «Отдел кадров» формировалось событие с низким уровнем нарушения.
10. Создать периметр «Конкуренты», внести туда почтовые домены и адреса электронной почты. Настроить политику с высоким уровнем нарушения и уведомлением офицеру безопасности по почте при отправке финансовой информации в данный периметр.
11. Создать шаблон почтового уведомления, который будет отправляться нарушителю в случае блокировки передачи грифов конфиденциальности на файлообменники.
12. Создать тестового пользователя с возможностью просмотра Сводки, просмотра и выполнения отчетов, запросов. Также данный пользователь должен видеть события только со средним уровнем нарушения.
13. Найти события почты, в которых было передано не более 5 вложений.
14. Найти события отправки по почте, на которые сработали одновременно политики «Грифованная информация», «Управление компанией».
15. Найти все события, где в теме письма указано «Информация только для служебного пользования».
16. Сформировать любой запрос и сделать так, чтобы были видны только следующие поля (дата перехвата, id события, отправитель, получатель, уровень нарушения). Отсортировать события по id события в порядке убывания.
17. Выгрузить события с вложениями, которые являются результатом выполнения пункта 14.
18. Создать новую панель сводки, внести туда следующие виджеты: Статистика по политикам, Динамика нарушений, Топ нарушителей, Количество нарушений за период и выгрузить ее.
19. Сделать так, чтобы в виджете Статистика по политикам отображались следующие политики «Грифованная информация», «Финансовая информация». А виджете топ нарушителей была статистика только по тем сотрудникам, которые имеют статус «Под подозрением».
20. Построить отчет, содержащий информацию о сотрудниках, которые являются активными пользователями социальных сетей и выгрузить ее в формате xls(x).

Практические задания по системе IW Device Monitor

1. Создать политику теневого копирования для почтовых сообщений, передаваемых по всем каналам с помощью протоколов SMTP, IMAP и назначить ее на группу компьютеров.
2. Создать политику, разрешающую только скачивание файлов со следующих облачных хранилищ: YandexDisk, OneDrive, DropBox и назначить ее на группу сотрудников.
3. Создать политику снятия теневой копии файлов, копируемых на съемные носители и при этом исключить файлы .tmp и назначить ее на группу компьютеров.
4. Создать политику, запрещающую использование приложения «Блокнот» и назначить ее на группу сотрудников.
5. Настроить на группу сотрудников перехват вставки из буфера обмена в следующие приложения: Microsoft Word, Adobe Reader, Microsoft Excel.

6. Запретить использование Skype и настроить контроль сообщений, передаваемых через Telegram для группы сотрудников.
7. Предоставить полный доступ к съемным устройствам хранения группе сотрудников на один день.
8. Настроить политику снятия скриншотов в случае запуска таких приложений, как Skype, Paint для определенной группы сотрудников.
9. Запретить для определенной группы компьютеров запуск любых приложений, помимо Skype.
10. Установить для определенной группы компьютеров сокрытие отображения уведомлений сотруднику.

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса

Требования к образованию и обучению лица, занимающего должность преподавателя: высшее образование - специалитет или магистратура, направленность (профиль) которого, как правило, соответствует преподаваемому учебному курсу, дисциплине (модулю).

Дополнительное профессиональное образование на базе высшего образования (специалитета или магистратуры) - профессиональная переподготовка, направленность (профиль) которой соответствует преподаваемому учебному курсу, дисциплине (модулю).

Педагогические работники обязаны проходить в установленном законодательством Российской Федерации порядке обучение и проверку знаний и навыков в области охраны труда.

Рекомендуется обучение по дополнительным профессиональным программам по профилю педагогической деятельности не реже чем один раз в три года.

Требования к опыту практической работы: при несоответствии направленности (профиля) образования преподаваемому учебному курсу, дисциплине (модулю) - опыт работы в области профессиональной деятельности, осваиваемой обучающимися или соответствующей преподаваемому учебному курсу, дисциплине (модулю).

Преподаватель: стаж работы в образовательной организации не менее одного года; при наличии ученой степени (звания) - без предъявления требований к стажу работы.

Особые условия допуска к работе: отсутствие ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации.

Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в порядке, установленном законодательством Российской Федерации

Прохождение в установленном законодательством Российской Федерации порядке аттестации на соответствие занимаемой должности.

Требования к материально-техническим условиям

Все занимаемые помещения соответствуют обязательным нормам пожарной безопасности и требованиям санитарно-эпидемиологических служб. Помещения имеют централизованные системы водоснабжения, отопления и канализации.

Образовательный процесс осуществляется с применением дистанционных образовательных технологий, с учетом чего созданы условия для функционирования электронной информационно-образовательной среды.

Требования к информационным и учебно-методическим условиям

Список литературы

1. InfoWatch Traffic Monitor Руководство администратора. https://kb.infowatch.com/pages/viewpage.action?pageId=179347699
2. InfoWatch Traffic Monitor Руководство пользователя. https://kb.infowatch.com/pages/viewpage.action?pageId=179348183
3. InfoWatch Device Monitor. Руководство пользователя https://kb.infowatch.com/pages/viewpage.action?pageId=173407089

Нормативные правовые акты

1. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ
2. «Конституция Российской Федерации» принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020
3. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ
4. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
6. Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ
7. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

Интернет-ресурсы

1. http://www.consultant.ru/
2. https://www.infowatch.ru/
3. https://habr.com/ru/all/
4. https://мойассистент.рф

ЗАКАЗЧИК:

_____

ИСПОЛНИТЕЛЬ:
ООО «АИВ»

Генеральный директор

_____ С.В. Харитонов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0238DBC800C9B04981437026D4A6E6EAF2
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 29.11.2023 до 28.02.2025