ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
Учебный центр «Профи групп»
ИНН 0278943664, ОГРН 1180280053854, E.mail pgroupp@mail.ru,
Тел. 8(347)246-36-02, г. Уфа, ул. Рабкоров, д.8/1, офис 3,4 этаж

УТВЕРЖДАЮ
Генеральный директор
ООО Учебный центр
«Профи Групп»
_____ А.П. Юдин
«___»_____ 20__г.

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Работа с документами, содержащими служебную информацию ограниченного распространения. Для сотрудников, которые имеют доступ к паспорту безопасности объекта и другим документам по вопросам антитеррористической безопасности»

Уфа 2024

Образовательная программа повышения квалификации «Работа с документами, содержащими служебную информацию ограниченного распространения. Для сотрудников, которые имеют доступ к паспорту безопасности объекта и другим документам по вопросам антитеррористической безопасности» – ООО Учебный центр «Профи групп», 2024 -25с.

Образовательная программа подготовлена преподавательским коллективом ООО Учебный центр «Профи групп».

Рекомендована Педагогическим советом
ООО Учебный центр «Профи групп»
«___» _____ 20__ г. Протокол № __

ОГЛАВЛЕНИЕ

1.ОБЩИЕ ПОЛОЖЕНИЯ

Образовательная программа разработана на основе следующих нормативных правовых актов Российской Федерации:

Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

Приказ Минобрнауки России от 01.07.2013 № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Федеральный закон от 06.03.2006 №35-ФЗ «О противодействии терроризму»

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности»

Указ Президента РФ от 15.02.2006 №116 «О мерах по противодействию терроризму»

Постановление Правительства РФ от 25.12.2013 №1244 «Об антитеррористической защищенности объектов (территорий)

Постановление Правительства РФ от 02.08.2019 №1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»

Постановление Правительства РФ от 06.03.2015 №202 «Об утверждении требований к антитеррористической защищенности объектов спорта и формы паспорта безопасности объектов спорта»

Постановление Правительства РФ от 11.02.2017 №176 «Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов»

Постановление Правительства РФ от 13.01.2017 №8 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»

Постановление Правительства РФ от 14.04.2017 №447 «Об утверждении требований к антитеррористической защищенности объектов (территорий) гостиниц и иных средств размещения и формы паспорта безопасности этих объектов»

Программа предназначена для обучения сотрудников, которые имеют доступ к паспорту безопасности объекта (территории) и другим документам по вопросам антитеррористической защищенности. Персонал этой категории проходит обязательную подготовку и переподготовку по работе со служебной информацией, в соответствии с требованиями нормативно-правовых актов в сфере применения Федерального закона от 06.03.2006 № 35-ФЗ «О

противодействии терроризму»

Требования к обучающимся:

наличие среднего профессионального и (или) высшего образования;

получение среднего профессионального и (или) высшего образования.

По работе со служебной информацией ограниченного распространения, содержащейся в паспорте безопасности объекта, обучение могут пройти руководители объектов, а также лица, допущенные к служебным сведениям. Ответственные лица, прошедшие подготовку, должны быть в следующих организациях: административных зданиях; общеобразовательных учреждениях, вузах, детских садах; торговых домах, супермаркетах, развлекательных центров; домах для детей-сирот, инвалидов, престарелых и других учреждения соцобслуживания; объектах сферы физической культуры и спорта — стадионах, дворцов спорта, спортклубах и так далее.

Целью реализации Программы является получение слушателями знаний, необходимых для совершенствования и повышению уровня комплексной безопасности объектов, а также углубленное изучение вопросов в области работы со служебной информацией ограниченного распространения, содержащейся в паспорте безопасности объекта и иных документах объекта.

Занятия проводятся по утвержденному графику на базе ООО Учебный центр «Профи групп» преподавательским составом.

Требования к условиям реализации программы.

При формировании и реализации образовательной программы ООО Учебный центр «Профи групп» обязан:

обеспечивать эффективную самостоятельную работу обучающегося в сочетании с совершенствованием управления ею со стороны педагогических работников;

способствовать развитию воспитательного компонента образовательного процесса.

Обучение по программе осуществляется по очной и заочной форме, при ее реализации применяются электронное обучение и дистанционные образовательные технологии.

Образовательная деятельность по программе осуществляется на государственном языке Российской Федерации.

Учебная деятельность обучающегося по программе может предусматривать следующие виды учебных занятий: лекции, практические занятия, консультации, определенные учебным планом программы.

Кадровое обеспечение реализации программы.

Реализация программы обеспечивается руководящими и педагогическими работниками ООО Учебный центр «Профи групп», а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

Педагогическую деятельность по программе должны осуществлять лица, имеющие высшее образование и отвечающие квалификационным требованиям, указанным в квалификационных справочниках, и (или)

профессиональным стандартам, а также прошедшие обучение по дополнительным профессиональным программам.

Информационно-методическое обеспечение учебного процесса при реализации программы.

Учебно-материальная база ООО Учебный центр «Профи групп» соответствует санитарно-гигиеническим и пожарно-техническим нормам и обеспечивает проведение всех видов занятий предусмотренных учебным планом программы.

Обучающийся в ООО Учебный центр «Профи групп» обеспечивается доступом к образовательной программе и методическим материалам образовательной организации, разработкам по ней, расписанию учебных занятий, к современным профессиональным базам данных, информационно-справочным и поисковым системам.

Обучающемуся по программе предоставлена возможность пользоваться библиотекой.

Кроме того, для обучающегося по программе организован доступ к полнотекстовым ресурсам электронной библиотеке.

Итоговое тестирование организуется и проводится либо через портал дистанционного обучения, либо путем письменных ответов на тестовые задания. Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование тем, разделов	Количество часов
1.	Основные понятия и нормативно-правовое регулирование антитеррористической защищенности объектов	12
2.	Организация деятельности по обеспечению антитеррористической защищенности и безопасности объектов (территорий)	12
3.	Обеспечение антитеррористической защищенности объекта	12
4.	Порядок разработки паспорта безопасности объекта	12
5.	Организация работы со служебной информацией ограниченного распространения	12
6.	Основы информационной безопасности	10
	Итоговая аттестация	**2**
	Итого	**72**

2.2. УЧЕБНАЯ ПРОГРАММА

Тема 1. Основные понятия и нормативно-правовое регулирование антитеррористической защищенности объектов

Термины и определения: объекты (территории), антитеррористическая защищенность (АТЗ) объекта, безопасность объектов (территорий), паспорт безопасности объекта (территории).

Постановления Правительства Российской Федерации от 2 августа 2019 г. N 1006, от 28 января 2019 г. N 52, от 11 февраля 2017 г. N 176, от 14 апреля 2017 г. N 447, от 13 января 2017 г. N 8, от 11 февраля 2017 г. N 176 и другие.

Приказ Министерства образования и науки РФ от 30 декабря 2010 г. N 2233.

Основные понятия и нормативно-правовое регулирование антитеррористической защищенности объектов

Основные понятия и нормативно-правовое регулирование работы с персональными данными

Требования к антитеррористической безопасности в образовательной организации. Обеспечение антитеррористической защищенности объекта

Пакет документов по антитеррористической безопасности в образовательной организации. Порядок разработки паспорта безопасности объекта

Тема 2. Организация деятельности по обеспечению антитеррористической защищенности и безопасности объектов (территорий)

Категорирование объектов (территорий). Категории опасности объектов (территорий). Инженерно-технические средства и системы обеспечения безопасности. Разработка, согласование и утверждение организационно-распорядительных документов организации по обеспечению АТЗ объекта (территории). Приказ о назначении должностных лиц, ответственных за проведение мероприятий по обеспечению АТЗ объектов (территорий) и организацию взаимодействия с территориальными органами безопасности, территориальными органами МВД РФ и территориальными органами Федеральной службы войск национальной гвардии РФ.

План мероприятий организации по исполнению требований нормативных актов по АТЗ. Приказ о мерах по защите информации при разработке и хранении паспорта безопасности и других документов, содержащих информацию ограниченного распространения.

Приказ об обследовании и категорировании объекта (территории) и разработке паспорта безопасности объекта (территории). Акт обследования и категорирования объекта (территории).

Перечень мероприятий по обеспечению АТЗ объекта (территории) инженернотехническими средствами и системами охраны. Паспорт безопасности объекта (территории). Положение (инструкция) об организации пропускного и внутриобъектового режимов. План действий при установлении уровней террористической опасности. План эвакуации работников, обучающихся и иных лиц, находящихся на объекте (территории), в случае

получения информации об угрозе совершения или о совершении террористического акта. План проведения учений и тренировок по отработке действий в условиях угрозы совершения или при условном совершении террористического акта на объекте (территории), связанных с эвакуацией обучающихся и персонала из помещений и зданий, которым угрожает опасность, а также обучением их способам индивидуальной и коллективной защиты. Журналы проведения инструктажа и практических занятий по действиям при обнаружении на объектах (территориях) посторонних лиц и подозрительных предметов, а также при угрозе совершения террористического акта.

Полномочия должностных лиц организации-правообладателя по обеспечению АТЗ объектов (территорий).

Тема 3. Обеспечение антитеррористической защищенности объекта

Противодействовать терроризму обязаны не только органы государственной и муниципальной власти. Обычные граждане, индивидуальные предприниматели и юридические лица должны организовать работу по предупреждению терроризма. Для этого необходимо обеспечить безопасность собственных или арендуемых зданий и сооружений.

Каждый объект должен быть максимально защищен от угрозы извне. Если это школа, директор принимает меры, чтобы террористы не проникли на территорию, а если такое произошло, чтобы помощь была вызвана мгновенно. Персонал должен знать свои действия на случай террористической угрозы, уметь оказать первую помощь пострадавшим.

Антитеррористическая защищенность объекта (далее — АТЗ) — состояние здания или территории, которое не позволит совершить террористический акт. Цель АТЗ — сберечь жизнь и здоровье людей, сохранность имущества, окружающей среды, флоры и фауны.

Чтобы обеспечить АТЗ, организация должна:

провести оценку уязвимости;

составить акт обследования;

категорировать объект защиты;

составить, согласовать паспорт безопасности и актуализировать его по мере необходимости;

отслеживать, как выполняется план по повышению защищенности, проводить ежегодные проверки.

Какие объекты подлежат антитеррористической защите

Согласно ч. 6 ст. 3 Закона «О противодействии терроризму» от 06.03.2006 № 35-ФЗ антитеррористической защищенности подлежат места массового пребывания, к которым относятся:

территории общего пользования поселения, муниципального округа или городского округа;

специально отведенные территории за их пределами;

места общего пользования в здании, строении, сооружении или ином объекте, на которых при определенных условиях может одновременно находиться более 50 человек.

В одной организации может быть несколько объектов защиты, если в каждом из зданий или строений находится одновременно больше 50 человек.

Какие нормативные акты регулируют эту сферу

Требования к антитеррористической защищенности объектов и территорий, их категории и формы паспортов безопасности утверждает Правительство РФ (п. 4 ч. 2 ст. 5 Федерального закона от 06.03.2006 № 35-ФЗ). Для разных сфер деятельности разработаны отдельные документы. Они содержат правила категорирования, формы паспортов безопасности и пр.

Категорию здания или территории устанавливают, опираясь на сведения о совершенных или предотвращенных террористических актах не только на самом объекте, но и в районе его расположения. Эта информация есть в сводках Федеральной службы безопасности, национальной гвардии, других статистических материалах.

Также для категоризации объектов защиты специалисты применяют математико-статистические методы расчета ущерба, с помощью которых можно оценить возможные потери населения и материального оснащения в случае террористического акта.

Чем выше категория риска, тем больше мероприятий предстоит выполнить руководству организации, чтобы обеспечить защиту.

Как организовать категорирование объекта

Критерии категорирования перечислены в постановлениях Правительства РФ. Единого набора не существует, к разным объектам применяются разные критерии, их выбор зависит от официальной статистики по предотвращенным терактам, прогнозных показателей по количеству пострадавших и материальному ущербу.

Чтобы правильно присвоить категорию, нужны статистические данные по совершенным или предотвращенным терактам — их необходимо получить в территориальном органе безопасности района расположения организации.

Прогнозный показатель количества пострадавших принимается равным максимальному количеству единовременно пребывающих людей на объекте или территории в рабочие дни. Прогнозный показатель материального ущерба — равным балансовой стоимости объекта или территории.

Критерии	Категория I	Категория II	Категория III	Категория IV
	Учреждение для отдыха и оздоровления детей (Постановление Правительства РФ от 14.05.2021 № 732)			
Количество попыток или совершенных терактов за последние 12 месяцев	Пять и более	От 3 до 4	До 2	Не зафиксировано терактов и попыток их совершения
Прогнозируемое количество пострадавших	Более 800 человек	От 300 до 800 человек	От 100 до 300 человек	Менее 100 человек
Прогнозируемый размер материального ущерба и ущерба окружающей природной среде	Более 300 млн руб.	От 300 до 150 млн руб.	От 75 до 150 млн руб.	Менее 75 млн руб.
	Объекты Минпросвещения (Постановление Правительства РФ от 02.08.2019 № 1006)			
Количество попыток или совершенных терактов за последние 12 месяцев	Показатели те же			
Прогнозируемое количество пострадавших	Более 1 100 человек	От 800 до 1100 человек	От 100 до 800 человек	Менее 100 человек
Прогнозируемый размер материального ущерба и ущерба окружающей природной среде	Показатели те же			Менее 15 млн руб.

Для того чтобы работа по АТЗ была систематизированной, руководитель предприятия должен разработать несколько документов. Первый — это план организационных и технических мероприятий по защищенности вверенных ему объектов с массовым пребыванием людей.

Организационные мероприятия:

Назначение ответственных за АТЗ.

Обучение и инструктажи по АТЗ, тренировки, обучение оказанию первой помощи пострадавшим при теракте; повышение квалификации для ответственных лиц и руководителя организации.

Заключение договоров с охранными предприятиями.

Категорирование мест массового пребывания людей с учетом степени потенциальной опасности и угрозы совершения на них террористического акта и его возможных последствий.

Разработка, утверждение, актуализация паспорта безопасности.

Технические мероприятия:

Установка систем контроля доступа на территорию, в здания и помещения.

Установка системы оповещения на случай террористического акта.

Оснащение объекта и территории инженерно-техническими средствами и системами охраны.

Приказ о создании комиссии, которая реализует этот план, обследует и присвоит объекту категорию риска, станет следующим документом. В комиссию кроме руководителя организации должны войти представители территориальных органов безопасности, МВД, Росгвардии.

В организации также должны быть:

Паспорт безопасности объекта или территории с перечнем мероприятий по обеспечению АТЗ. Это основной документ, подлежащий проверке. Его составляют с учетом присвоенной категории риска, сроков реализации мероприятий, объема планируемых работ и выделенных средств на два финансовых года, следующих за текущим.

Приказ о мерах по защите информации при разработке и хранении паспорта безопасности.

План взаимодействия с территориальными органами безопасности, МВД РФ, Росгвардии. Нужен, потому что система антитеррористической защиты не может существовать обособленно. Она должна соответствовать характеру деятельности, быть интегрированной в систему управления предприятием.

Положение (инструкция) об организации пропускного и внутриобъектового режимов и план действий при установлении уровней террористической опасности.

Нужна обучающая работа с персоналом организации и посетителями. Если речь идет о школе, то каждый ученик должен знать план эвакуации в случае сигнала угрозы теракта.

Проводите плановые учения и тренировки по отработке правильных действий. Всех работников и посетителей известите о правилах эвакуации, применении средств индивидуальной и коллективной защиты, месте сбора при эвакуации. Для этой цели нужно проводить инструктажи по АТЗ. Уделите внимание отработке действий при условном совершении террористического акта. Проводите устные опросы, записи о них вносите в журналы проведения инструктажа и практических занятий.

Для реализации всех планов, включая тренировки, оснащение СКУД, взаимодействие с ведомствами и пр., необходимо назначить ответственных. Они вместе с руководителем организации должны пройти повышение квалификации по АТЗ.

Нельзя назначать ответственными тех, кто не обладает административно-управленческим ресурсом. Полномочия зафиксируйте в должностных инструкциях сотрудников, формулировки вы найдете в отраслевых постановлениях Правительства РФ.

Примеры должностных обязанностей

Руководитель организации: вести общее руководство обеспечением АТЗ; утверждать паспорта безопасности объектов; анализировать эффективность системы защищенности.

Заместитель руководителя организации: планировать мероприятия по обеспечению АТЗ объектов и территорий; обеспечивать мероприятия по АТЗ ресурсами; координировать деятельность подразделений и должностных лиц организации по обеспечению АТЗ объектов (территорий); организовывать взаимодействие с территориальными органами безопасности, МВД, МЧС, Росгвардии.

Ответственный за обеспечение АТЗ объектов: разрабатывать и согласовывать проекты локальных нормативных актов в части обеспечения АТЗ объектов и территорий; координировать совместные действия с территориальными органами безопасности, МВД, МЧС, Росгвардии; участвовать в планировании и выполнении мероприятий по обеспечению АТЗ; проводить инструктажи и обучения по АТЗ.

Руководитель структурного подразделения: руководить мероприятиями по АТЗ объектов и территорий в соответствии с требованиями и организационно-распорядительными документами предприятия.

Обучение работников и посетителей объекта, например учеников школы или пациентов больницы, проводится по программам, которые не отличаются от программ обучения оказанию первой помощи пострадавшим на производстве. Составляются они на основе Приказа Минздравсоцразвития России от 04.05.2012 № 477н.

Первая помощь при терактах нужна в следующих ситуациях:

отсутствие сознания;

остановка дыхания и кровообращения;

наружные кровотечения;

инородные тела в верхних дыхательных путях;

травмы различных областей тела;

ожоги, эффекты воздействия высоких температур, теплового излучения;

обморожение и другие эффекты воздействия низких температур;

отравление.

Чтобы обучить работников и посетителей, организация должна приобрести и подготовить технические средства: тренажеры, учебные пособия, плакаты, стенды, памятки.

Как оформить акт обследования и категорирования объекта

Акт обследования и категорирования объекта защиты — это первый этап создания паспорта безопасности. Акт составляют в двух экземплярах. Как и паспорту безопасности, ему присваивают гриф «ДСП» (для служебного пользования) или гриф секретности. Выбор зависит от категории объекта (ст. 8 Закона РФ от 21.07.1993 № 5485-1).

Категорирование проводят в момент ввода объекта в эксплуатацию и в случае значимых изменений его характеристик, например при монтаже новой автоматической системы пожаротушения.

Каждый федеральный орган исполнительной власти (министерство, ведомство), в ведении которого находятся организации, разрабатывает методический материал, который помогает составлять акт обследования и категорировать объекты защиты.

Акт обследования и категорирования объекта защиты составляет комиссия, назначенная приказом руководителя организации. Требования к созданию комиссии в органах исполнительной власти различны. Во всех случаях можно привлекать сотрудников органов безопасности и МВД России.

В некоторых ведомствах допустимо привлекать:

сотрудников специализированных организаций;

экспертов специализированных организаций, у которых есть право проводить экспертизу безопасности объектов (территорий);

работников организаций, специализирующихся в области инженерно-технического оборудования объектов, проектирования и монтажа технических средств охраны;

экспертов в области проектирования и эксплуатации технологических систем.

Каких-либо нормативно закрепленных прямых ограничений или запретов, кроме конфиденциальности информации, по составу комиссии нет. Собственник должен в первую очередь защищать информацию, представляющую интерес для террористов.

Ответственность за неисполнение законодательных требований

Многие работодатели, к сожалению, халатно относятся к обеспечению АТЗ, притом что ужесточены меры ответственности за неисполнение законодательных требований — вплоть до уголовной ответственности.

В конце 2019 года в КоАП РФ появилась ст. 20.35, которая предусматривает ответственность за нарушения антитеррористического законодательства для объектов и территорий.

За нарушения организациям грозит штраф от 100 000 до 500 000 руб., должностным лицам — дисквалификация от полугода до трех лет или штраф от 30 000 до 50 000 руб.

Если действия виновных будут содержать признаки уголовного преступления, наступят основания для уголовного преследования конкретного человека — руководителя организации или сотрудника, который по должности занимался обеспечением безопасности и антитеррористической защищенности.

В этой ситуации директор школы и его заместитель по безопасности могут быть привлечены к уголовной ответственности по ч. 3 ст. 293 УК РФ за халатность, которая привела к гибели людей. А это принудительные работы на срок до пяти лет, а также в некоторых случаях лишение права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. Второй вариант — лишение свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Тема 4. Порядок разработки паспорта безопасности объекта

Сроки проведения категорирования и паспортизации объектов (территорий). Порядок экспертной оценки состояния антитеррористической защищенности и безопасности объектов (территорий), организация и проведение обследования и категорирования объектов (территорий). Порядок участия членов комиссии в проведении экспертной оценки состояния антитеррористической защищенности и безопасности охраняемого объекта (территории). Оформление результатов обследования объекта (территории). Разработка паспорта безопасности объекта (территории). Согласование. Актуализация паспорта безопасности объекта (территории).

Паспорт безопасности состоит из обязательных разделов:

Общие сведения об объекте (территории). Это сведения из устава организации, ЕГРЮЛ/ЕГРИП, кадастрового паспорта.

Сведения о работниках, обучающихся и иных лицах, находящихся на объекте (территории). Укажите среднее количество сотрудников

и посетителей, сведения о площади объекта и режиме работы организации, например количество смен.

Сведения о критических элементах объекта (территории). Это важная информация, которая опирается на вероятностные методы. Критические элементы — это потенциально опасные элементы объекта, незаконное вмешательство в которые приведет к нарушению функционирования объекта.

Прогноз последствий в результате совершения на объекте (территории) террористического акта.

Оценка социально-экономических последствий совершения террористического акта. Этот раздел заполняется на основе бухгалтерских данных с учетом стоимости активов.

Силы и средства, привлекаемые для обеспечения антитеррористической защищенности объекта (территории). Укажите, кто охраняет объект: частное охранное предприятие или войска Росгвардии.

Меры по инженерно-технической, физической защите и пожарной безопасности объекта. Перечислите, какие автоматические системы оповещения и связи, средства пожаротушения применяются на объекте.

Выводы и рекомендации.

Дополнительные сведения с учетом особенностей объекта (территории).

Тема 5. Организация работы со служебной информацией ограниченного распространения

Прием, учет (регистрация), размножение (тиражирование), пересылка, хранение, уничтожение документов, содержащих служебную информацию ограниченного распространения.

Взаимодействие с территориальными органами безопасности, территориальными органами Министерства внутренних дел Российской Федерации, территориальными органами Федеральной службы войск национальной гвардии Российской Федерации. Обеспечение защиты служебной информации ограниченного распространения, содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации, в том числе служебной информации ограниченного распространения о принимаемых мерах по антитеррористической защищенности объекта (территории).

Установление порядка работы со служебной информацией ограниченного распространения.

Ограничение доступа должностных лиц (работников) к служебной информации ограниченного распространения, содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации. Определение обязанностей лиц, допущенных к служебной информации ограниченного распространения, в том числе лиц, ответственных за хранение паспорта безопасности объекта (территории), иных документов и других материальных носителей информации, содержащих сведения о состоянии антитеррористической защищенности объекта (территории) и принимаемых мерах по ее усилению.

Обеспечение надлежащего хранения и использования служебной информации ограниченного распространения, в том числе содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации.

Организация и осуществление контроля за обеспечением установленного порядка работы со служебной информацией ограниченного распространения и ее хранения в целях выявления и предупреждения возможной утечки служебной информации ограниченного распространения, в том числе содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации.

Подготовка и переподготовка должностных лиц (работников) по вопросам работы со служебной информацией ограниченного распространения

Тема 6. Основы информационной безопасности

В основе информационной безопасности лежит обеспечение информации-акт поддержания конфиденциальности, целостности и доступности информации (ЦРУ), гарантирующий, что информация никоим образом не будет скомпрометирована при возникновении критических проблем. Эти проблемы включают, но не ограничиваются ими, стихийные бедствия, неисправность компьютера/сервера и физическую кражу.

Информационная безопасность, или ИБ, — это комплекс мер, которые нужны, чтобы защитить от утечки или взлома программы, компьютерные системы и данные. Еще так называют отрасль, которая занимается этими мерами.

Самый простой пример меры по информационной безопасности — антивирус, установленный на компьютере. Но в коммерческих структурах к этому вопросу подходят более серьезно и на многих уровнях: чтобы обеспечить безопасность, нужно много чего сделать

Средства информационной безопасности защищают данные от утечки, программы, системы и сети — от взлома, несанкционированного доступа, порчи файлов или других видов атак. Если речь о коммерческих или государственных структурах, сведения также защищают от шпионов или возможных злоумышленников внутри самого коллектива.

Информационная безопасность защищает системы от проникновения и от атак. Сюда входит не только взлом: это и DDoS-атаки, в результате которых может «лечь» сервер сайта, и утечка данных, и многое другое. Злоумышленников намного больше, чем кажется. И никто не хочет, чтобы их сервис потерял работоспособность, а данные оказались доступны всем вокруг. Для этого и нужна информационная безопасность.

У компаний есть еще одна причина: за утечку конфиденциальных данных пользователей они несут ответственность по закону. Так что для них меры по безопасности — это еще и способ избежать проблем с законодательством и потери доверия клиентов.

Без мер по информационной безопасности кто угодно мог бы получить доступ к конфиденциальным сведениям или взломать любой сайт или систему. Компьютерным пространством стало бы фактически невозможно пользоваться.

Информационная и кибербезопасность охватывают различные области, имеют разные цели. Но есть и общие черты.

Информационная безопасность — это более широкая категория защиты, которая включает криптографию, мобильные вычисления и социальные сети. Она связана с защитой информации от угроз, не связанных с человеком. Например, сбоев серверов или стихийных бедствий.

Кибербезопасность охватывает только цифровые данные и интернет-угрозы. Также кибербезопасность включает защиту необработанных, несекретных данных, а информационная безопасность — нет.

Угрозы безопасности разделяют на две категории: внутренние и внешние.

Внутренние. Это угрозы, которые идут изнутри системы. Чаще всего в таких случаях речь идет об утечке данных или об их повреждении. Например, кто-то подкупил сотрудника, и тот похитил данные, составляющие коммерческую тайну. Второй вариант — злоумышленником оказался авторизованный пользователь.

Еще одна внутренняя угроза — риск банальной ошибки, в результате которой конфиденциальные сведения окажутся в открытом доступе или повредятся. Например, в открытом доступе оказалась часть базы данных или пользователь по неосторожности повредил файлы. Такое уже бывало в истории. А нужно, чтобы таких случаев не возникало: клиент не мог бы нарушить работу системы даже случайно, а информация оставалась защищена.

Внешние. Сюда относятся угрозы, которые приходят извне, и они могут быть куда разнообразнее. Это, например, попытка взлома системы через найденную уязвимость: злоумышленник проникает в сеть, чтобы украсть или повредить информацию. Или DDoS-атака, когда на веб-адрес приходит огромное количество запросов с разных адресов, и сервер не выдерживает, а сайт перестает работать.

Сюда же можно отнести деятельность компьютерных вирусов: они способны серьезно навредить работе системы. Действия таких вредоносных программ могут быть очень разнообразными: от рассылки спама от имени взломанного адреса до полной блокировки системы и повреждения файлов.

Еще к внешним угрозам безопасности относятся форс-мажоры и несчастные случаи. Например, хранилище данных оказалось повреждено в результате аварии или пожара. Такие риски тоже нужно предусмотреть.

Кто работает с информационной безопасностью

Существует отдельная должность специалиста по информационной безопасности. В крупных компаниях это может быть отдельный департамент. В маленьких — один сотрудник, причем порой он также выполняет обязанности системного администратора или сетевого инженера. Бывает и так, что информационную безопасность отдают на аутсорс: в этом случае ею занимаются сотрудники специализированной компании.

В широком смысле простейшие меры по информационной безопасности предпринимает кто угодно. Установить антивирус и блокировщик навязчивой рекламы, не посещать подозрительные сайты и не запускать непроверенные файлы — все это тоже меры ИБ, хоть и максимально простые. Но настоящий специалист по безопасности — это профессионал с широкими знаниями и множеством специфических навыков.

Три принципа информационной безопасности

Информационная безопасность отвечает за три вещи: доступность, конфиденциальность и целостность данных. Сейчас расскажем, что это означает.

Доступность. Это значит, что к информации могут получить доступ те, у кого есть на это право. Например, пользователь может зайти в свой аккаунт и увидеть все, что в нем есть. Клиент может перейти в каталог и посмотреть на товары. Сотрудник может зайти во внутреннюю базу данных для его уровня доступа. А если на систему производится атака и она перестает работать, доступность падает порой до полного отказа.

Конфиденциальность. Второй принцип — конфиденциальность. Он означает, что информация должна быть защищена от людей, не имеющих права ее просматривать. То есть в тот же аккаунт пользователя не сможет войти чужой человек. Без регистрации нельзя комментировать что-то на сайте, без личного кабинета — оплатить заказ. Человек, который не работает в компании, не может зайти в ее внутреннюю сеть и посмотреть там на конфиденциальные данные. Если систему взламывают, конфиденциальность оказывается нарушенной.

Целостность. Целостность означает, что информация, о которой идет речь, не повреждена, существует в полном объеме и не изменяется без ведома ее владельцев. Комментарий не сможет отредактировать посторонний человек — только автор или иногда модератор. Сведения в базе данных меняются только по запросу тех, у кого есть доступ. А в вашем аккаунте не появятся письма, написанные от вашего лица без вашего ведома. При взломе системы целостность опять же может нарушиться: информацию могут модифицировать

Какие данные охраняет ИБ

Персональные. Персональные данные — информация, которая связана с какими-то людьми. Это ФИО, телефон, адрес жительства, электронная почта и многое другое. По российским законам эти данные нужно охранять от несанкционированного доступа. Поэтому компании спрашивают разрешение на обработку персональных данных, если вы регистрируетесь на сайтах или заказываете какие-то услуги. Они обязаны это делать. А потом — хранить эту информацию, чтобы к ней не получили доступ чужие люди.

Истории про нарушение конфиденциальности этих данных вы наверняка слышали. Например, мошенники могут звонить клиентам банков, а их номера получают из слитых баз. Вот пример того, к чему может привести недостаточная информационная безопасность.

Тайные. Еще одна категория сведений — те, которые составляют тайну: государственную, коммерческую, профессиональную и служебную.

К гостайне относятся сведения, важные для безопасности страны, и они засекречены максимально строго. Коммерческая тайна — информация, критичная для нормальной работы компании: если она раскроется, организация может потерять деньги или конкурентное преимущество. При этом компания не имеет право засекречивать некоторые сведения: имена владельцев, условия труда и так далее.

Отдельно стоят профессиональная и служебная тайна. Профессиональная тайна — это, например, врачебная: история болезни пациента не должна раскрываться посторонним людям, как и данные о его состоянии. А еще — адвокатская, нотариальная и некоторые другие. А служебная тайна — некоторая информация, которая принадлежит определенным службам, например налоговой.

Все эти сведения нужно защищать: их утечка или повреждение способны причинить серьезные проблемы.

Общедоступные. Не удивляйтесь. Информация, которая известна всем, все еще должна быть доступной и целостной. Поэтому ее тоже следует защищать, иначе кто угодно сможет изменить цену товара в интернет-магазине и подставить этим покупателей. Или «уронить» сайт, чтобы никто не смог на него войти.

В каких сферах ИБ важнее всего

Есть отрасли, для которых защита информации очень важна, так как потеря данных способна нанести им катастрофический ущерб. Обычно это сферы, которые работают с деньгами или с другими ценностями.

Банки и финансы. Банковские сервисы относятся к безопасности очень строго. Защищать информацию здесь нужно не только от возможных взломщиков, но и от мошенников, и от других злоумышленников. Поэтому банки обычно защищены на очень высоком

уровне. Даже для авторизации в личном кабинете с незнакомого устройства нужны дополнительные действия: сначала система проверит, что вы — это вы.

Государственные сервисы. Второй случай крайне важных данных — государственные сервисы и системы. Если это внутренняя сеть, в ней могут храниться сведения, составляющие государственную тайну, а ее утечка — прямая угроза безопасности страны. А в сервисах для граждан множество персональной информации: паспортные данные, сведения о работе, штрафах, семье и многом другом. Потеря таких сведений поставит под удар огромный процент населения.

Компании с большой базой персональных данных. Это различные крупные сервисы, в которых зарегистрировано много людей. Если их персональные данные «утекут», кто угодно сможет воспользоваться ими в своих целях — а компания будет нести за это ответственность.

Важные сектора экономики. Энергетические, нефтегазовые и другие предприятия тоже должны быть хорошо защищены. В системах таких структур есть информация, которая составляет коммерческую тайну, и в этом случае она критична. Более того, оборудованием и механизмами тоже может управлять автоматика, цифровая система. Если кто-то получит к ней доступ, то сможет застопорить всю работу предприятия.

Дата-центры. Это помещения, где стоит и работает серверное оборудование. К их оснащению и доступу к ним предъявляются повышенные требования, чтобы сервера были защищены от внешних воздействий и от различных угроз. В том числе от злоумышленников: в случае с физическим оборудованием украсть или повредить информацию может быть довольно просто. Поэтому нужно не допустить, чтобы кто-либо в принципе получил несанкционированный доступ к помещению.

Электронная коммерция. Интернет-магазины и другие сайты, которые работают с платежами пользователей, тоже должны заботиться о безопасности — по понятным причинам. Утечка платежных данных — это очень серьезно и может привести к потере денег.

Какими методами пользуются специалисты по ИБ

Какую информацию нужно защищать и зачем — разобрались. Теперь поговорим о том, как именно это делают. Информационная безопасность — это не одно действие, а целый набор разнообразных мер:

поиск технических уязвимостей и защита от них;

«защита от дурака», чтобы никто не смог навредить данным по ошибке;

создание инфраструктуры, которая устойчива к частым способам атаки;

шифрование информации внутри сети или системы;

защита паролей и других конфиденциальных сведений;

защита базы данных от несанкционированного вмешательства;

контроль доступа людей к критичной информации;

предоставление доступа по защищенным каналам;

отслеживание поведения пользователей, чтобы вовремя пресечь возможную угрозу;

построение системы оповещений об уязвимостях и взломах;

регулярное проведение аудитов, которые описывают состояние системы.

И это только малая часть возможных действий, причем за каждым из них скрывается огромная и разнообразная работа.

Специалист по информационной безопасности работает с определенными инструментами — они помогают защитить сведения от посягательств. Их условно можно разделить на физические, технические и административные.

Физические. Это инструменты, которые существуют в физическом мире. К ним обычно относится различное оборудование. Пластиковые ключи-карты и замки, которые открываются по ним, — это физический инструмент. Установленные в дата-центре резервные сервера — тоже. Еще сюда можно отнести видеонаблюдение и сигнализацию, использование сейфов, работу с физическими источниками информации, мониторинг оборудования и многое другое.

Технические и программные. Это то, что относится скорее к софту, а не к железу, от защищенных протоколов до антивируса. Шифрование данных, передача сведений через HTTPS, установка брандмауэра и так далее — такие меры. Есть и специальные инструменты: защитное ПО и сервисы, программы для поиска уязвимостей и имитации атак, многое другое. К техническим средствам еще можно отнести построение инфраструктуры защищенной системы и сети.

Некоторые компании называют техническими средствами все, что связано с техникой. Это ярко видно, например, в официальных документах, даже если фактически они описывают физические методы.

Административные. Сюда относится построение внутренней инфраструктуры, регламенты и контроль доступа. Например, разработка матрицы доступа — документа, который определяет, какие полномочия есть у каждого сотрудника. Эти меры защищают не от технических угроз, а скорее от человеческого фактора. Так человек без соответствующих полномочий не сможет получить доступ к конфиденциальным данным.

Как начать заниматься информационной безопасностью

На «личном», персональном уровне обеспечить себе защиту не так сложно. Нужно пользоваться брандмауэром и антивирусом, посещать сайты только с защищенным соединением, не скачивать подозрительный контент.

Другое дело — стать специалистом по информационной безопасности. Это куда сложнее: профессия комплексная, требует большого количества разнородных знаний. Понадобится изучить, как функционируют системы и сети, знать об основных уязвимостях и атаках, уметь их закрывать и отражать. Более того, специалист по ИБ должен сам уметь атаковать системы: это важно, например, при пентесте. Желательно знать некоторые языки программирования, и точно нужно знать внутренние языки для управления ОС.

На курсах мы дадим вам представление о том, как стать ИБ-шником, и поможем стартовать в этой сложной, но интересной отрасли.

3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Федеральный закон от 6 марта 2006 г. N 35-ФЗ "О противодействии терроризму".

2. Указ Президента Российской Федерации от 15 февраля 2006 г. N 116 "О мерах по противодействию терроризму".

3. Постановление Правительства Российской Федерации от 27 мая 2017 г. N 638 "О взаимодействии федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, физических и юридических лиц при проверке информации об угрозе совершения террористического акта, а также об информировании субъектов противодействия терроризму о выявленной угрозе совершения террористического акта".

4. Постановление Правительства РФ от 14 апреля 2017 г. N 447 "Об утверждении требований к антитеррористической защищенности гостиниц и

иных средств размещения и формы паспорта безопасности этих объектов".

5. Постановление Правительства РФ от 14 мая 2021 г. N 732 "Об утверждении требований к антитеррористической защищенности объектов (территорий), предназначенных для организации отдыха детей и их оздоровления, и формы паспорта безопасности объектов (территорий) стационарного типа, предназначенных для организации отдыха детей и их оздоровления".

6. Постановление Правительства РФ от 13 января 2017 г. N 8 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)".

7. Постановление Правительства РФ от 11 февраля 2017 г. N 176 "Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)".

8. Постановление Правительства РФ от 28 января 2019 г. N 52 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства спорта Российской Федерации и подведомственных ему организаций, а также формы паспорта безопасности объектов (территорий) Министерства спорта Российской Федерации и подведомственных ему организаций".

9. Постановление Правительства РФ от 19 октября 2017 г. N 1273 "Об утверждении требований к антитеррористической защищенности торговых объектов (территорий) и формы паспорта безопасности торгового объекта (территории)". 8

10. Постановление Правительства РФ от 19 апреля 2019 г. N 471 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства транспорта Российской Федерации, Федерального агентства воздушного транспорта, Федерального агентства железнодорожного транспорта, Федерального агентства морского и речного транспорта, Федерального дорожного агентства, Федеральной службы по надзору в сфере транспорта, их территориальных органов, а также подведомственных им организаций и формы паспорта безопасности этих объектов (территорий)".

11. Приказ Минрегиона РФ от 5 июля 2011 г. N 320 "Об утверждении свода правил "Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования" (вместе с "СП 132.13330.2011. Свод правил. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования").

12. Приказ МЧС России от 25 октября 2004г. № 484 «Об утверждении типового паспорта безопасности территорий субъектов Российской Федерации и муниципальных образований».

4. ФОРМЫ АТТЕСТАЦИИ

Ответственность за реализацию программы в полном объеме в соответствии с примерным учебным планом, качество подготовки обучающегося несет ООО Учебный центр «Профи групп».

Контроль успеваемости обучающегося - важнейшая форма контроля образовательной деятельности, включающая в себя целенаправленный систематический мониторинг освоения обучающимся программы в целях:

получения необходимой информации о выполнении обучающимся учебного плана программы;

оценки уровня знаний, умений, навыков и приобретенной обучающимся компетенции.

Оценка качества освоения программы включает текущий контроль успеваемости обучающегося, промежуточную и итоговую аттестацию.

Результаты контроля успеваемости, промежуточной и итоговой

аттестаций вносятся в журнал учета занятий, успеваемости, посещаемости обучающихся, экзаменационные (зачетные) ведомости (экзаменационные (зачетные) листы.

Порядок организации и проведения текущего контроля успеваемости обещающихся определяется ООО Учебный центр «Профи групп» самостоятельно.

Освоение программы завершается итоговой аттестацией, которая проводится в порядке, установленным соответствующим локальным нормативным актом ООО Учебный центр «Профи групп».

Итоговая аттестация для обучающегося проводится в соответствии с требованиями, установленными Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

Для организации и проведения итоговой аттестации, допуска обучающегося по программе к ней и принятия решения о присвоении квалификации в образовательной организации формируется аттестационная комиссия.

К итоговой аттестации приказом Генерального директора ООО Учебный центр «Профи групп» допускается лицо, не имеющее академической задолженности и выполнившее требования, предусмотренные учебным планом программы.

Итоговая аттестация проводится в сроки, предусмотренные учебным планом и расписанием учебных занятий.

Результаты итоговой аттестации объявляются в день окончания ее проведения.

Оценка качества освоения программы осуществляется аттестационной комиссией, состав которой утверждается приказом Генерального директора ООО Учебный центр «Профи групп».

Лицу, не прошедшему итоговую аттестацию, а также лицу, освоившему часть программы и (или) исключенному из списков обучающихся образовательной организации в ходе освоения программы, выдается справка об обучении установленного образца.