УТВЕРЖДЕН
постановлением
Правительства
Хабаровского края
от 20 февраля 2019 г. № 48-пр

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых органами исполнительной власти Хабаровского края, аппаратом Губернатора и Правительства Хабаровского края

№ п/п	Угрозы безопасности информации*			
	идентификатор угроз безопасности информации	наименование	описание	источник угрозы (характеристика и потенциал нарушителя)
1	2	3	4	5
1.	6	Угроза внедрения кода или данных	угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устройство вредоносного кода, который может быть в дальнейшем запущен "вручную" пользователями, автоматически при выполнении определенного условия (наступления определенной даты, входа пользователя в систему) или с использованием аутентификационных данных, заданных "по умолчанию", а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов, и блокирования работы устройства при выполнении определенных команд. Данная угроза обусловлена: - наличием уязвимостей программного обеспечения; - слабостями мер антивирусной защиты и разграничения доступа к защищаемым ресурсам; - наличием открытого Telnet-порта на IoT-устройстве (только для IoT-устройств).	внешний нарушитель с низким потенциалом

1	2	3	4	5
			Реализация данной угрозы возможна: - в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; - при наличии у дискредитируемого пользователя привилегий установки программного обеспечения; - в случае неизмененных владельцем учетных данных IoT-устройства (заводских пароля и логина)	
2.	8	Угроза восстановления аутентификационной информации	угроза заключается в возможности подбора (например, путем полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учетной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объемом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: - время подбора в основном определяется не объемом аутентификационной информации, а объемом данных ее хеш-кода; - восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях "вручную"	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
3.	15	Угроза доступа к защищаемым файлам с использованием обходного пути	угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях: - наличие у нарушителя прав доступа к некоторым объектам файловой системы; - отсутствие проверки вводимых пользователем данных; - наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с ее помощью	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
4.	28	Угроза использования альтернативных путей доступа к ресурсам	угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных.	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом

1	2	3	4	5
			Реализация данной угрозы возможна при условии наличия у нарушителя: - возможности ввода произвольных данных в адресную строку; - сведений о пути к защищаемому ресурсу; - возможности изменения интерфейса ввода входных данных	
5.	30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учетной записи "по умолчанию" дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учетные записи "по умолчанию", предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной "по умолчанию" после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: - наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учетной записи "по умолчанию" для объекта защиты; - успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты	внешний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом
6.	31	Угроза использования механизмов авторизации для повышения привилегий	угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учетных записей с более высокими чем у нарушителя привилегиями, за счет ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
7.	41	Угроза межсайтового скриптинга	угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую информационную систему	внешний нарушитель с низким потенциалом
8.	46	Угроза нарушения процедуры	угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия.	внешний нарушитель с низким потенциалом, внут-

1	2	3	4	5
		аутентификации субъектов виртуального информационного взаимодействия	Данная угроза обусловлена наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между ее уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия	ренний нарушитель с низким потенциалом
9.	59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Данная угроза обусловлена уязвимостями программного обеспечения уровня управления виртуальной инфраструктурой, реализующего функцию распределения компьютерных ресурсов между пользователями. Реализация данной угрозы возможна при условии успешного осуществления нарушителем несанкционированного доступа к программному обеспечению уровня управления виртуальной инфраструктурой, реализующему функцию распределения компьютерных ресурсов между пользователями	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
10.	62	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключенный к браузеру в качестве плагина. Данная угроза обусловлена слабостями механизма контроля доступа к настройкам браузера. Реализация возможна в случае успешного осуществления нарушителем включения режима использования прозрачного прокси-сервера в параметрах настройки браузера, например, в результате реализации угрозы межсайтового скриптинга	внешний нарушитель с низким потенциалом
11.	67	Угроза неправомерного ознакомления с защищаемой информацией	угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего ее использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путем просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путем подслушивания разговоров	внутренний нарушитель с низким потенциалом
12.	69	Угроза неправомерных действий в каналах связи	угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путем добавления или удаления данных из информационного потока в целях оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи.	внешний нарушитель с низким потенциалом

1	2	3	4	5
			Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	
13.	71	Угроза несанкционированного восстановления удаленной защищаемой информации	угроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удаленная с машинного носителя, в большинстве случаев может быть восстановлена. Реализация данной угрозы возможна при следующих условиях: - удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных (например, физическое уничтожение машинного носителя информации); - технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; - информация не хранилась в криптографически преобразованном виде	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
14.	74	Угроза несанкционированного доступа к аутентификационной информации	угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации. Данная угроза обусловлена наличием слабостей мер разграничения доступа к защищаемой информации. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа к участкам оперативного или постоянного запоминающего устройства, в которых хранится информация аутентификации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
15.	75	Угроза несанкционированного доступа к виртуальным каналам передачи	угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путем некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
16.	78	Угроза несанкционированного доступа к	угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации.	внешний нарушитель с низким потенциалом, внутренний наруши-

1	2	3	4	5
		защищаемым виртуальным машинам из виртуальной и (или) физической сети	Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия	тель с низким потенциалом
17.	79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
18.	84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путем логического объединения нескольких виртуальных устройств хранения данных). Данная угроза обусловлена наличием слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и (или) виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны с высокой сложностью алгоритмов обеспечения согласованности действий по распределению информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства. Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабости технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации)	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
19.	86	Угроза несанкционированного изменения аутентификационной информации	угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учетной записью дискредитированного пользователя	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
20.	87	Угроза несанкциони-	угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI.	внешний нарушитель с высоким

1	2	3	4	5
		рованного использования привилегированных функций BIOS	Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала	потенциалом, внутренний нарушитель с низким потенциалом
21.	88	Угроза несанкционированного копирования защищаемой информации	угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путем проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съемный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
22.	89	Угроза несанкционированного редактирования реестра	угроза заключается в возможности внесения нарушителем изменений в используемый дискредитируемым приложением реестр данных (далее – реестр), которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы Microsoft Windows, а любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью. Данная угроза обусловлена слабостями механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром. Реализация данной угрозы возможна в случае получения нарушителем прав на работу с программой редактирования реестра	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
23.	90	Угроза несанкционированного создания учетной записи пользователя	угроза заключается в возможности создания нарушителем в системе дополнительной учетной записи пользователя и ее дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учетной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удаленном доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
24.	91	Угроза несанкционированного удаления за-	угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путем осуществления деструктивного программного или физического воздействия на машинный носитель информации.	внешний нарушитель с низким потенциалом, внутренний наруши-

1	2	3	4	5
		щищаемой информации	Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующем данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	тель с низким потенциалом
25.	98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы ("сканирование портов") для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика	внешний нарушитель с низким потенциалом
26.	99	Угроза обнаружения хостов	угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика	внешний нарушитель с низким потенциалом
27.	116	Угроза перехвата данных, передаваемых по вычислительной сети	угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном или активном режиме ("прослушивание сетевого трафика") для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в следующих условиях:	внешний нарушитель с низким потенциалом

1	2	3	4	5
			- наличие у нарушителя доступа к дискредитируемой вычислительной сети; - неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	
28.	128	Угроза подмены доверенного пользователя	угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять прием/передачу данных от его имени. Данную угрозу можно охарактеризовать как "имитация действий клиента". Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации. Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств, типе используемого программного обеспечения	внешний нарушитель с низким потенциалом
29.	156	Угроза утраты носителей информации	угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или ее потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учета носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	внутренний нарушитель с низким потенциалом
30.	159	Угроза "форсированного веб-браузинга"	угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищенные компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации "ручного ввода" в адресную строку веб-браузера определенных адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	внешний нарушитель с низким потенциалом
31.	167	Угроза заражения компьютера при посещении неблагонадежных сайтов	угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадежным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадежным содержимым	внутренний нарушитель с низким потенциалом
32.	168	Угроза "кражи" учетной	угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путем получения информации идентификации/аутен-	внешний нарушитель с низким по-

1	2	3	4	5
		записи доступа к сетевым сервисам	тификации, соответствующей учетной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам), с которой связан неактивный/несуществующий адрес электронной почты. Данная угроза обусловлена недостаточностью мер контроля за активностью/существованием ящиков электронной почты. Реализация данной угрозы возможна при условиях: - наличия статуса "свободен для занимания" у адреса электронной почты, с которым связана учетная запись доступа пользователя к сетевым сервисам (например, если пользователь указал при регистрации несуществующий адрес или долго не обращался к почтовому ящику, вследствие чего его отключили); - наличия у нарушителя сведений об адресе электронной почты, с которым связана учетная запись дискредитируемого пользователя для доступа к сетевым сервисам	тенциалом
33.	170	Угроза неправомерного шифрования информации	угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа. Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа. Реализация данной угрозы возможна при условии успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации, а также успешного обнаружения (идентификации) нарушителем защищаемых файлов	внешний нарушитель с низким потенциалом
34.	171	Угроза скрытного включения вычислительного устройства в состав бот-сети	угроза заключается в возможности опосредованного осуществления нарушителем деструктивного воздействия на информационные системы с множества вычислительных устройств (компьютеров, мобильных технических средств), подключенных к информационно-телекоммуникационной сети "Интернет" (далее – сеть Интернет), за счет захвата управления такими устройствам путем несанкционированной установки на них: - вредоносного программного обеспечения типа Backdoor для обеспечения нарушителя возможностью удаленного доступа/управления дискредитируемым вычислительным устройством; - клиентского программного обеспечения для включения в ботнет и использования созданного таким образом ботнета в различных противоправных целях (рассылка спама, проведение атак типа "отказ в обслуживании"). Данная угроза обусловлена уязвимостями в сетевом программном обеспечении и слабостями механизмов антивирусного контроля и межсетевого экранирования. Реализация данной угрозы возможна при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет	внешний нарушитель с низким потенциалом
35.	172	Угроза распространения "почтовых червей"	угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа "почтовый червь", а также невольного участия в дальнейшем противоправном распростра-	внешний нарушитель с низким потенциалом

1	2	3	4	5
			нении вредоносного кода. Данная угроза обусловлена слабостями механизмов антивирусного контроля. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя электронного почтового ящика, а также наличия в его адресной книге хотя бы одного адреса другого пользователя	
36.	173	Угроза "спама" веб-сервера	угроза заключается в возможности неправомерного осуществления нарушителем массовой рассылки коммерческих, политических, мошеннических и иных сообщений на веб-сервер без запроса со стороны дискредитируемых веб-серверов. Данная угроза обусловлена уязвимостями механизмов фильтрации сообщений, поступающих из сети Интернет. Реализация данной угрозы возможна при условии наличия в дискредитируемом веб-сервере активированного функционала, реализующего различные почтовые сервера, службы доставки мгновенных сообщений, блоги, форумы, аукционы веб-магазинов, онлайн-сервисы отправки SMS-сообщений, онлайн-сервисы голосования	внешний нарушитель с низким потенциалом
37.	174	Угроза "фарминга"	угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией, в том числе идентификации/аутентификации, пользователя путем скрытного перенаправления пользователя на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию. Данная угроза обусловлена уязвимостями DNS-сервера, маршрутизатора. Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; - средств создания и запуска поддельного сайта; - специальных программных средств типа "эксплойт", реализующих перенаправление пользователя на поддельный сайт. Кроме того, угрозе данного типа подвержены подлинные сайты, не требующие установления безопасного соединения перед вводом информации ограниченного доступа	внешний нарушитель с низким потенциалом
38.	175	Угроза "фишинга"	угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией, в том числе идентификации/аутентификации, пользователя путем убеждения его с помощью методов социальной инженерии, в том числе посылкой целевых писем ("spear-phishing attack"), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений ("fake offers") или различных приложений ("fake apps"), зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть зараженное вложение в письме. Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах "фишинга".	внешний нарушитель с низким потенциалом

1	2	3	4	5
			Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; - средств создания и запуска поддельного сайта; - сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.). Для убеждения пользователя раскрыть информацию ограниченного доступа (или открыть вложение в письме) наиболее часто используются поддельные письма от администрации какой-либо организации, с которой взаимодействует пользователь (например, банк)	
39.	178	Угроза несанкционированного использования системных и сетевых утилит	угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему за счет использования имеющихся или предварительно внедренных стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети). Реализация данной угрозы возможна при условиях: - наличия в системе стандартных системных и сетевых утилит или успешного их внедрения нарушителем в систему и сокрытия (с использованием существующих архивов, атрибутов "скрытый" или "только для чтения"); - наличия у нарушителя привилегий на запуск таких утилит	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
40.	180	Угроза отказа подсистемы обеспечения температурного режима	угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа входящих в нее подсистем вентиляции и температурных приборов	внешний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом
41.	186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода посредством рекламы, сервисов и (или) контента (убеждения пользователя системы активировать ссылку, код) при посещении пользователем системы сайтов в сети Интернет или установки программ с функцией показа рекламы. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов в сети Интернет	внутренний нарушитель с низким потенциалом
42.	191	Угроза внедрения вредоносного кода	угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты.	внешний нарушитель с низким потенциалом, внут-

1	2	3	4	5
		в дистрибутив программного обеспечения	Реализация данной угрозы возможна при: - применении пользователем сторонних дистрибутивов; - отсутствии антивирусной проверки перед установкой дистрибутива	ренний нарушитель с низким потенциалом
43.	192	Угроза использования уязвимых версий программного обеспечения	угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
44.	208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	угроза заключается в возможности использования вычислительных ресурсов средств вычислительной техники для осуществления сторонних вычислительных процессов. Угроза реализуется за счет внедрения в средства вычислительной техники вредоносной программы, содержащей код, реализующий использование вычислительных ресурсов для своих нужд (в частности, для майнинга криптовалюты). Данная угроза обусловлена недостаточностью следующих мер защиты информации: - мер по антивирусной защите, что позволяет выполнить установку и запуск вредоносной программы; - мер по ограничению программной среды, что позволяет нарушителю осуществлять бесконтрольный запуск программных компонентов	внешний нарушитель с низким потенциалом, внешний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом, внутренний нарушитель со средним потенциалом
45.	209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	угроза заключается в возможности получения доступа к защищенной памяти из программы, не обладающей соответствующими правами, в результате эксплуатации уязвимостей, позволяющих преодолеть механизм разграничения доступа, реализуемый центральным процессором	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом
46.	211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспе-	угроза заключается в возможности деструктивного воздействия на информационную систему и обрабатываемую ею информацию в результате работы программного обеспечения, используемого для администрирования информационных систем	внутренний нарушитель с низким потенциалом

1	2	3	4	5
		чением администрирования информационных систем		

*Угрозы безопасности с учетом содержания персональных данных, характера и способов их обработки в информационных системах персональных данных уточняются операторами информационных систем персональных данных – органами исполнительной власти края в частных моделях угроз безопасности персональных данных в соответствии с Описанием информационных систем персональных данных, эксплуатируемых органами исполнительной власти Хабаровского края, аппаратом Губернатора и Правительства Хабаровского края, и рекомендациями по определению актуальных угроз безопасности персональных данных в них согласно приложению к настоящему Перечню.